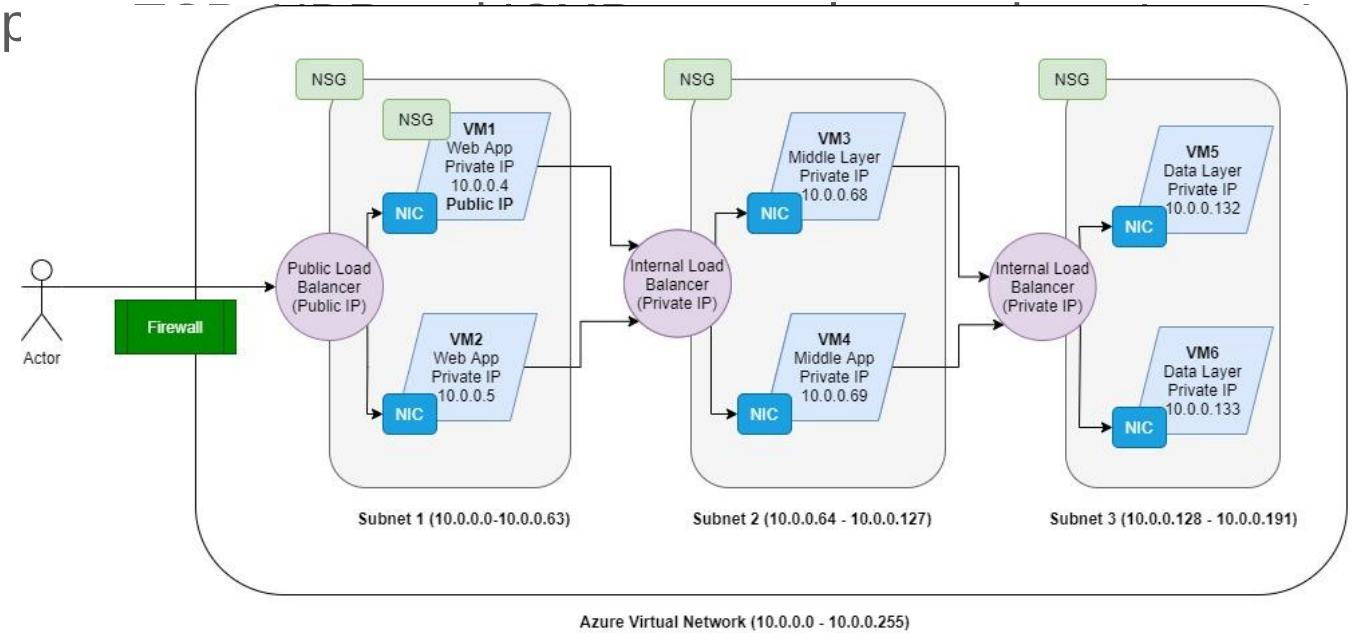
Configuring Network Security Group

Agenda

- Understand NSG Default Rules
- Configure Rules
    - HTTP rule
    - RDP rule
- NSG Flows

Network Security Group

- Set of rules that handles the inbound and outbound traffic
- Applied at subnet or NIC level
- Supp



greatlearning
Learning for Life

Virtual Network Security

Agenda

- Azure Bastion
- Azure Firewall
- DDos protection

greatlearning
Learning for Life

Virtual Networking

Agenda

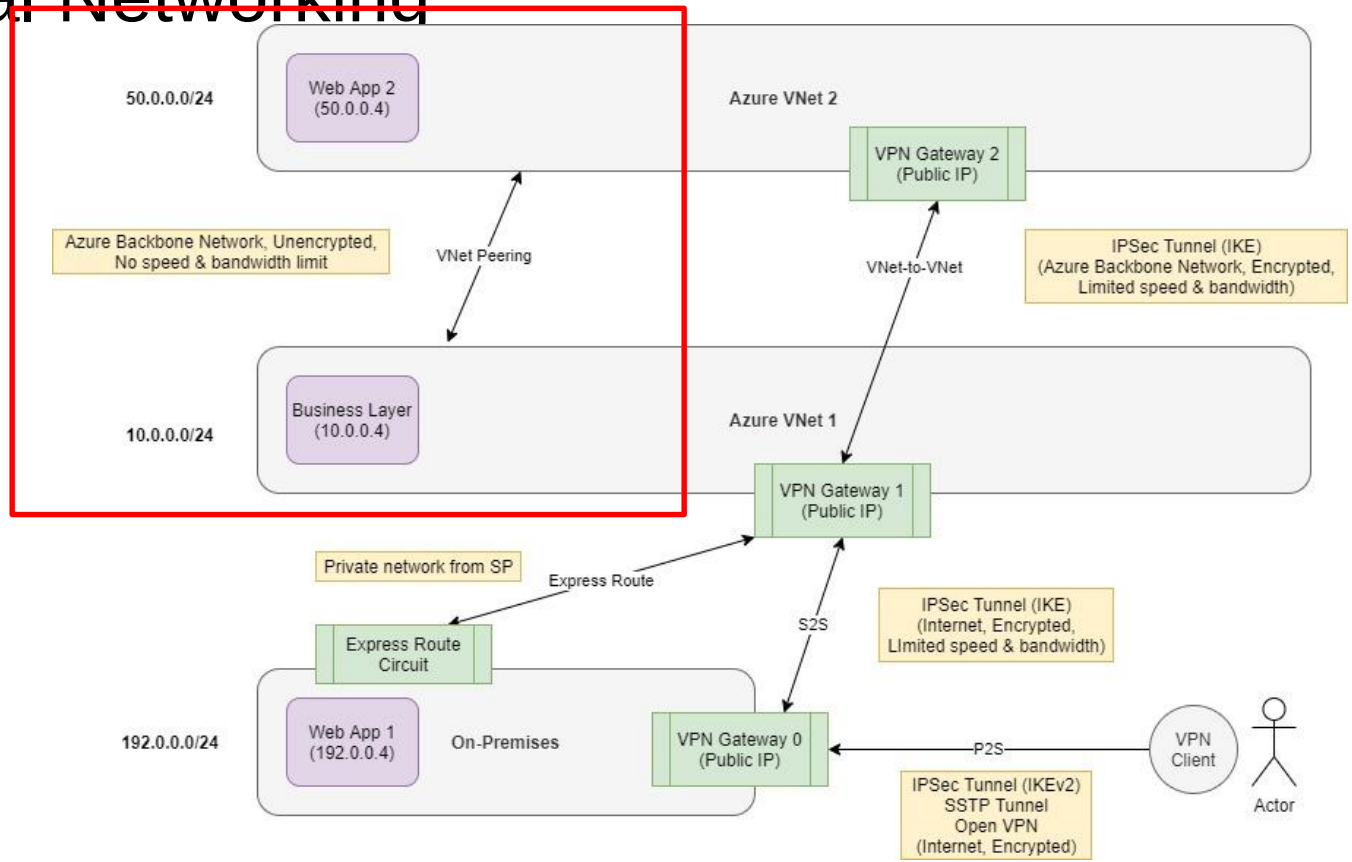
- Connectivity between different networks
  - Point-to-Site
  - Site-to-Site
  - VNet-to-VNet
  - VNet Peering
  - Express Route

Virtual Network Peering

Agenda

- Setup VNet Peering
    - Ping VM in VNet1 from VM in VNet2
- Hub-and-spoke network topology using VNet Peering

Virtual Networking

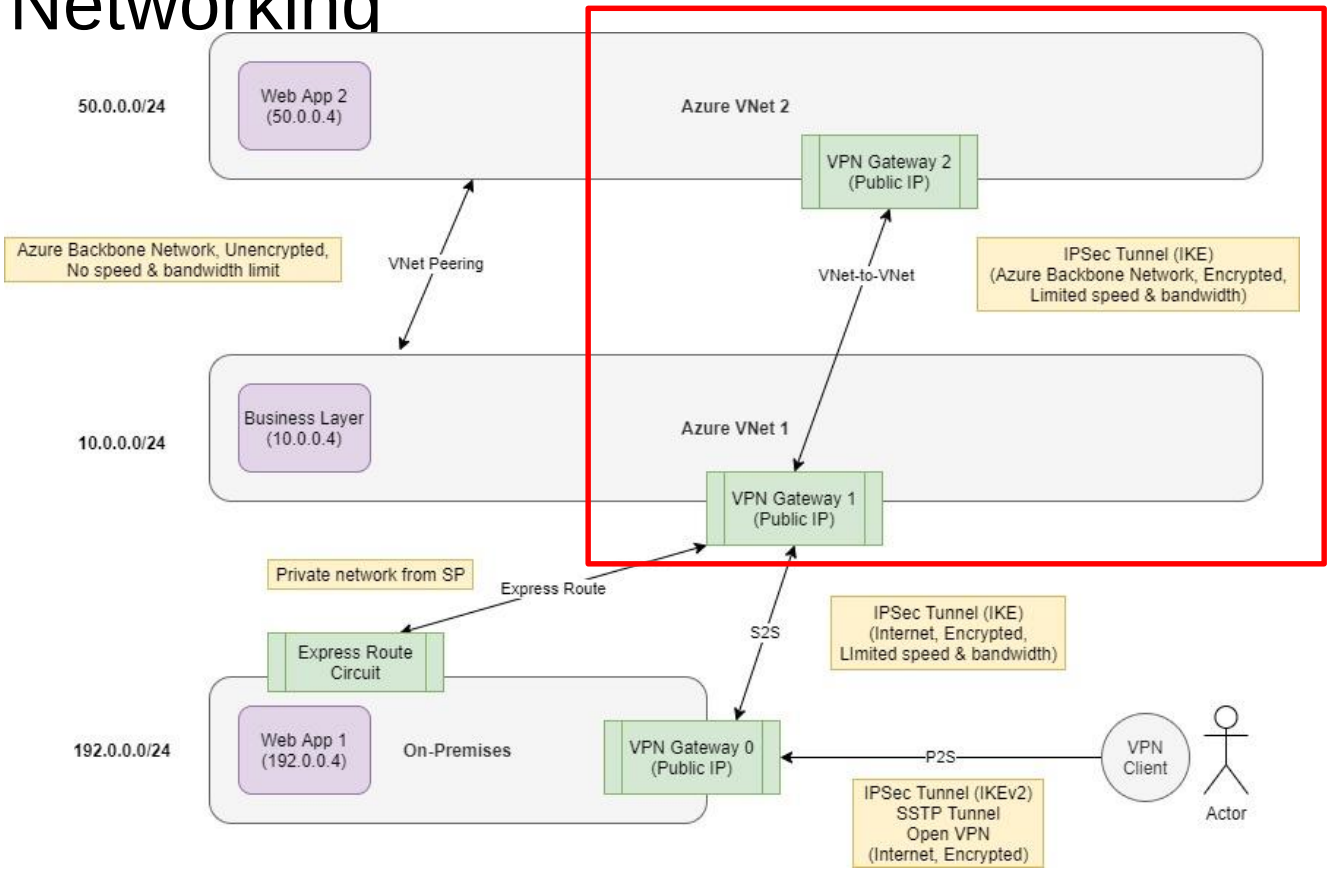


VNet-to-VNet Connectivity

Agenda

- Setup VPN Gateway
- Configure VNet-to-VNet connectivity

Virtual Networking



Azure Load Balancer - Introduction

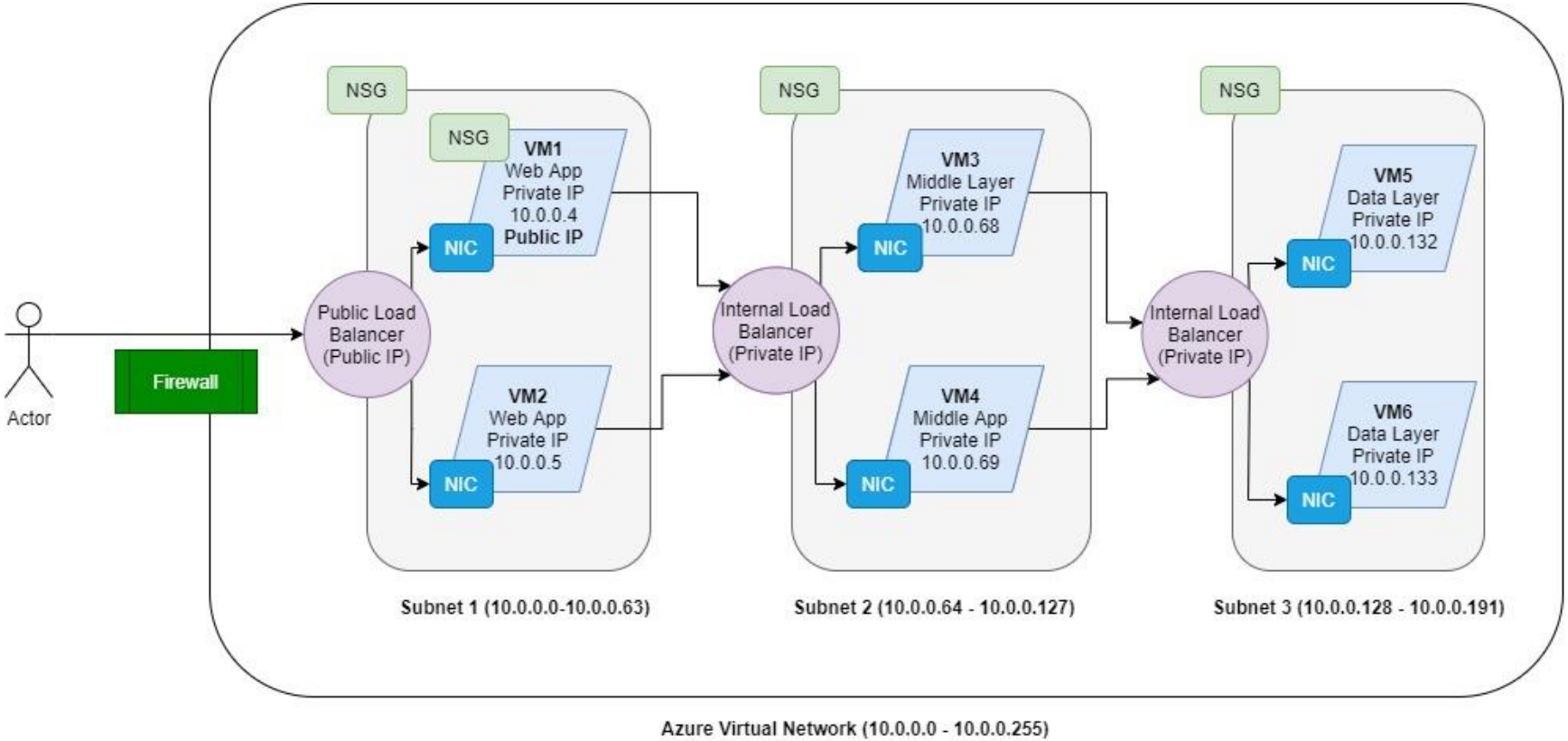
Agenda

- What is Azure Load Balancer?
- Load Balancer Types
- Types of Rules
- Load Balancing Rule
    - Components
    - Algorithms

Azure Load Balancer

- Distributes inbound traffic to backend VMs for scalability and HA
- Works at Layer 4 of OSI stack - TCP and UDP protocols
- Can be used for internet facing (public) and internal applications
- Supports multiple applications using multiple IP addresses and ports
- Backend VMs must be in the same Virtual Network
    - VMs can be in different Availability Zones
- Supports both inbound and outbound scenarios
    - Can configure NAT and SNAT rules
- Supports IPv6 addresses

N-Tier Architecture



Load Balancer Types

- Public Load Balancer
  - Public IP address must be specified for Load Balancer
  - Handles traffic from internet to backend VMs
  - Backend VMs do not require Public IP addresses
  - Outbound traffic from VM is translated from private IP of VM to public IP of Load Balancer

- Internal Load Balancer
  - Deployed inside Virtual Network
  - It can be accessed over a private IP address

greatlearning
Learning for Life

Azure Load Balancer - Advanced

Agenda

- Inbound NAT Rules
- Floating IP
- Outbound NAT Rules
- Load Balancer SKUs

SKUs Comparison

Basic SKU

- Supports max 300 VMs
- Supports VMs in either one Availability Set or one Virtual Machine Scale Set
- No SLA guaranteed
- Health probe protocols – TCP and HTTP
- Preconfigured outbound rules
- Multiple Frontends for inbound traffic only

Standard SKU

- Supports max 1000 VMs
- Supports VMs from one virtual network (use multiple Availability Sets or Scale Sets)
- 99.99% SLA
- Health probe protocols – TCP, HTTP, HTTPS
- Configurable outbound rules
- Multiple Frontends for inbound & outbound traffic

greatlearning
Learning for Life

Azure Application Gateway

Agenda

- What is Azure Application Gateway?
- Components
- Features

Azure Application Gateway

- Web traffic load balancer to handle traffic for web applications
- Works at Layer 7 of OSI stack - HTTP and HTTPS protocols
- Can be used for internet facing (public) and internal applications
- Application layer routing – route traffic based on URL
- Redirect traffic to backend VMs / VM Scale Sets / Azure App Services / external sites
- Web Application Firewall (WAF) to protect apps from web vulnerabilities
- Use it together with other Load Balancing services

Features

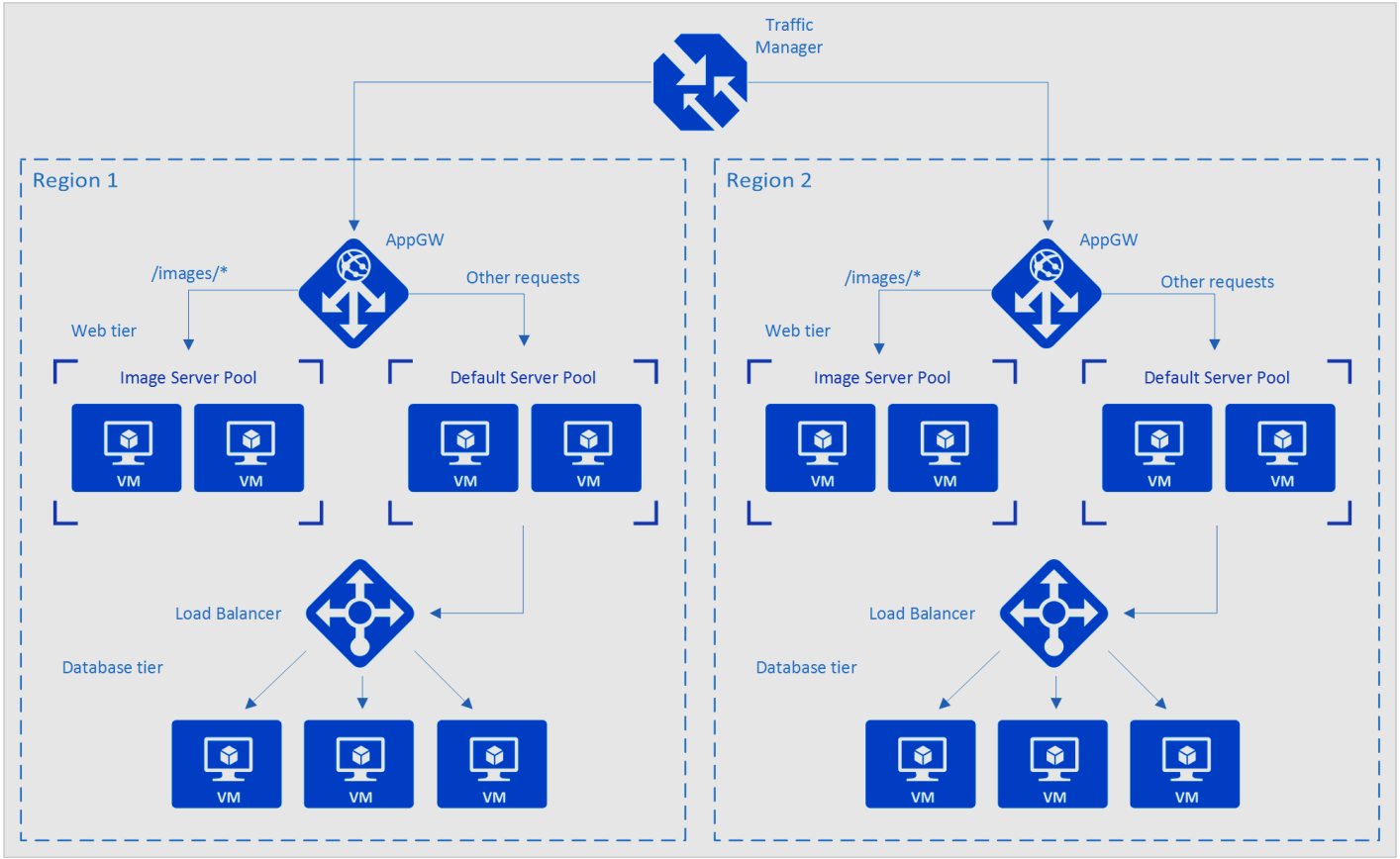
- Zone redundancy
- Autoscaling support
- Static Frontend IP
- Multiple backend resource types – VM, VMSS, App Services, IP Address
- Session affinity and connection draining
- Multiple listeners and multiple-site support
- Redirection support
- Path-based routing
- Rewrite HTTP headers and URL
- Custom error pages
- SSL/TLS termination and end-to-end SSL/TLS support
- Web Application Firewall (WAF) support

Azure Traffic Manager

Agenda

- What is Azure Traffic Manager?
- How it works?
- Routing Methods

Combining Load Balancing Services

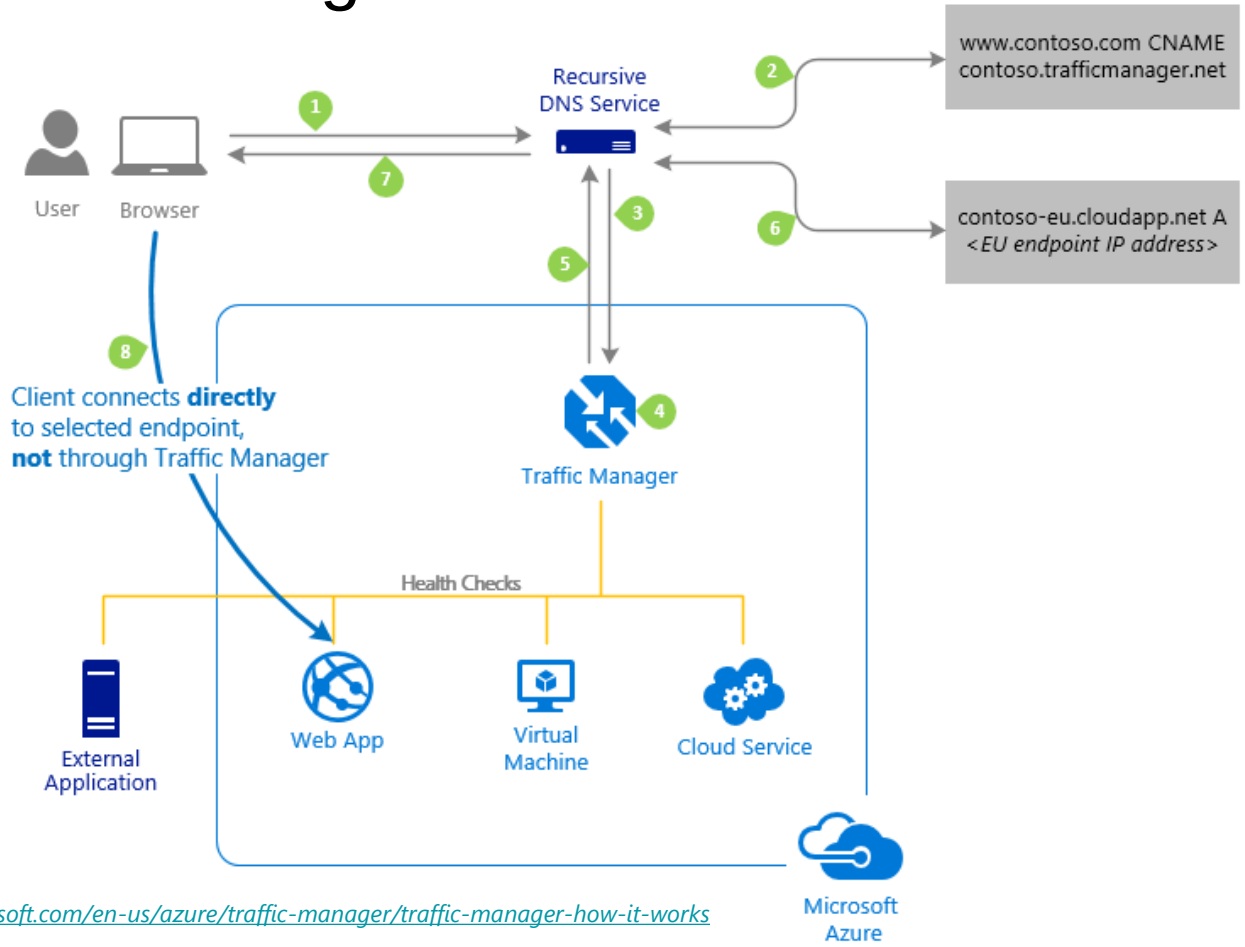


Source: https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-load-balancing-azure

Azure Traffic Manager

- DNS-based load balancer
- Directs the client request to an endpoint, based on DNS
- Works at global level. Not deployed in a region
- Multiple endpoint support
    - Azure services (App Services, VMs)
    - External endpoints (IP address, domain names etc.)
    - Another Azure Traffic Manager
- Endpoints can be in any region / location
- Use routing method to select the endpoint where traffic is to be diverted
- Use it together with other Load Balancing services

How Traffic Manager Works?

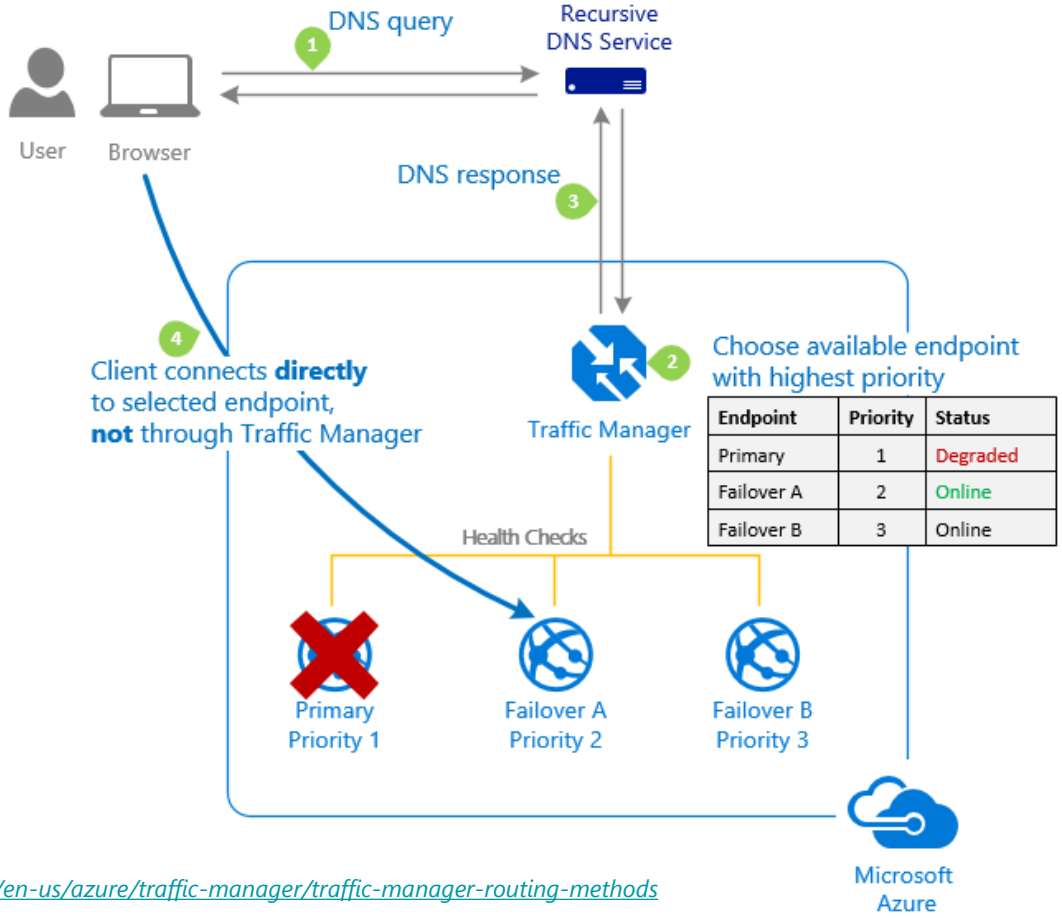


Source: https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-how-it-works

Routing Methods

- Performance
- Priority
- Weighted
- Geographic
- Multivalue
- Subnet

Routing Method - Priority

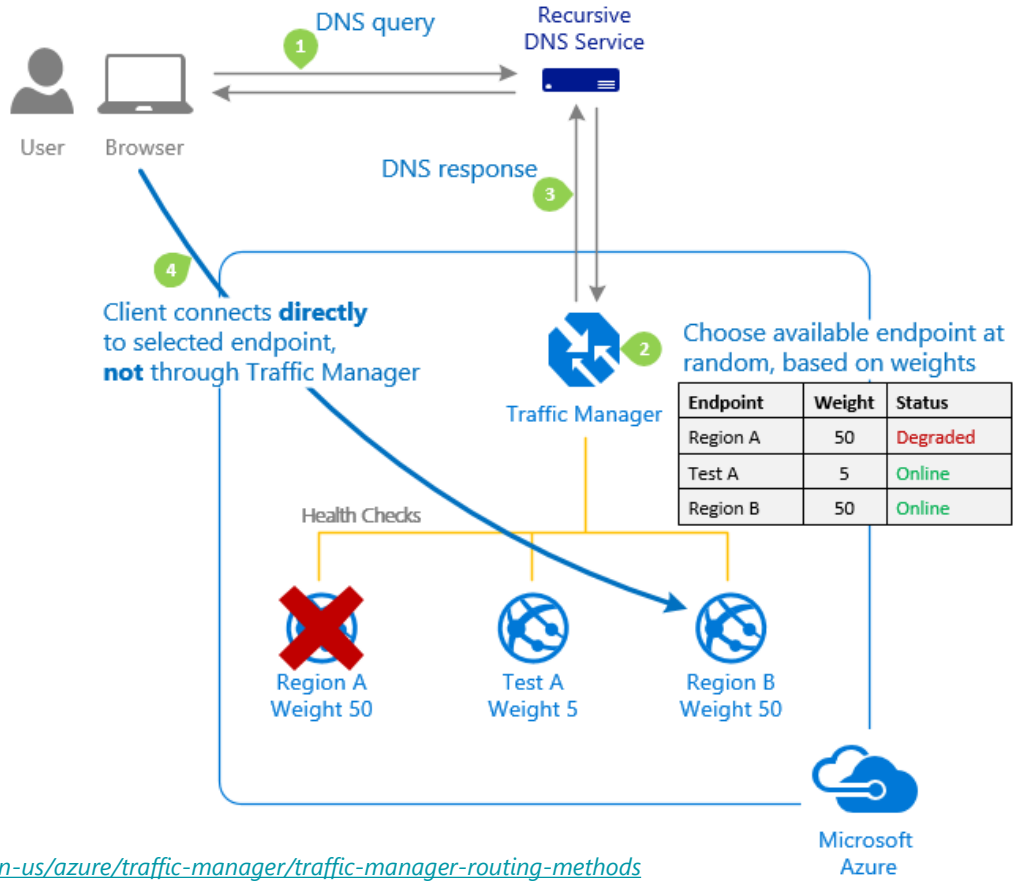


Source: https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods

Routing Method - Priority

- Each endpoint is assigned a priority between 1 to 1000
- Endpoint with highest priority gets all the traffic
- Lower priority number = Higher priority
- In case highest priority endpoint goes down, then traffic goes to next endpoint in the priority list
- Benefits
    - Allows to design Failover pattern

Routing Method - Weighted

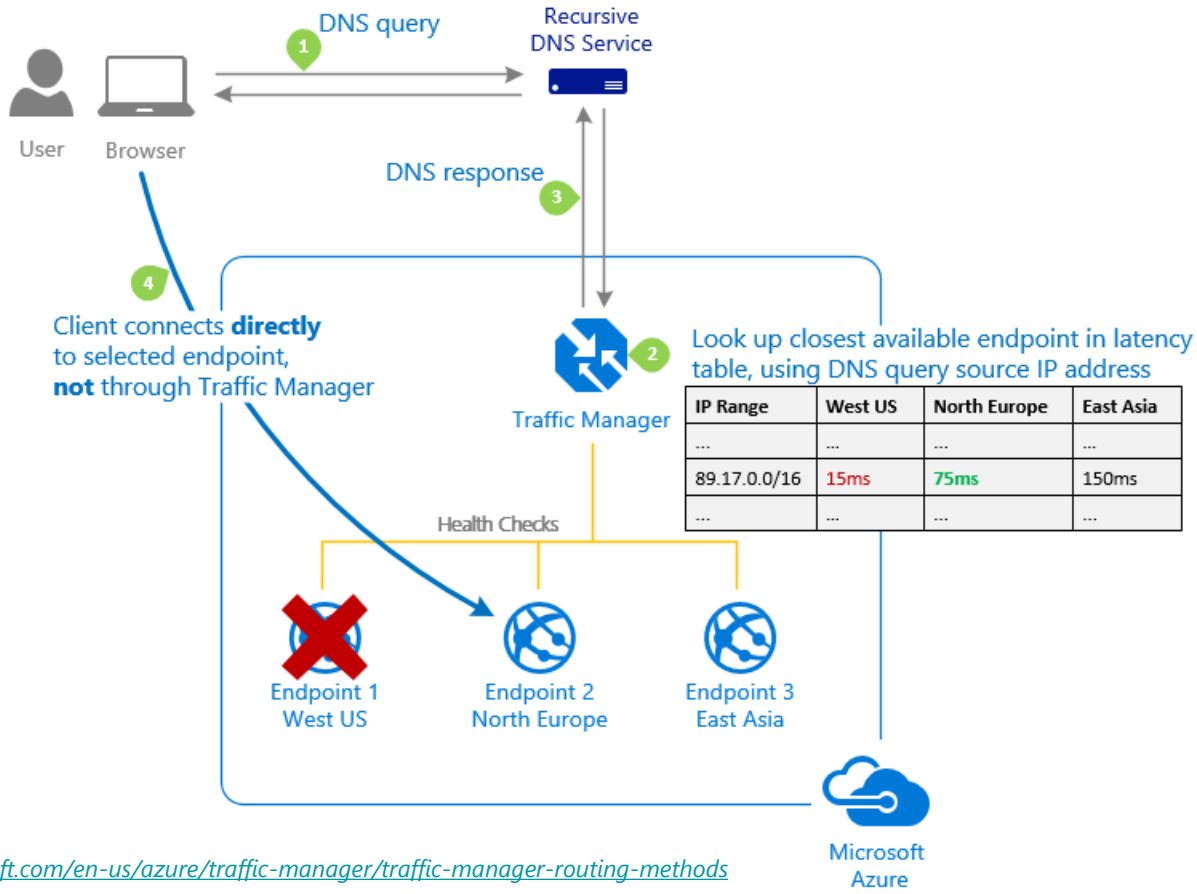


Source: https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods

Routing Method - Weighted

- Each endpoint is assigned a weight between 1 to 1000
- Default weight value is 1
- Traffic is distributed based on the weight of endpoint
- Higher weight = More traffic
- Benefits
    - Endpoints with higher capacity can be given more traffic
    - Upgrading an application gradually

Routing Method - Performance

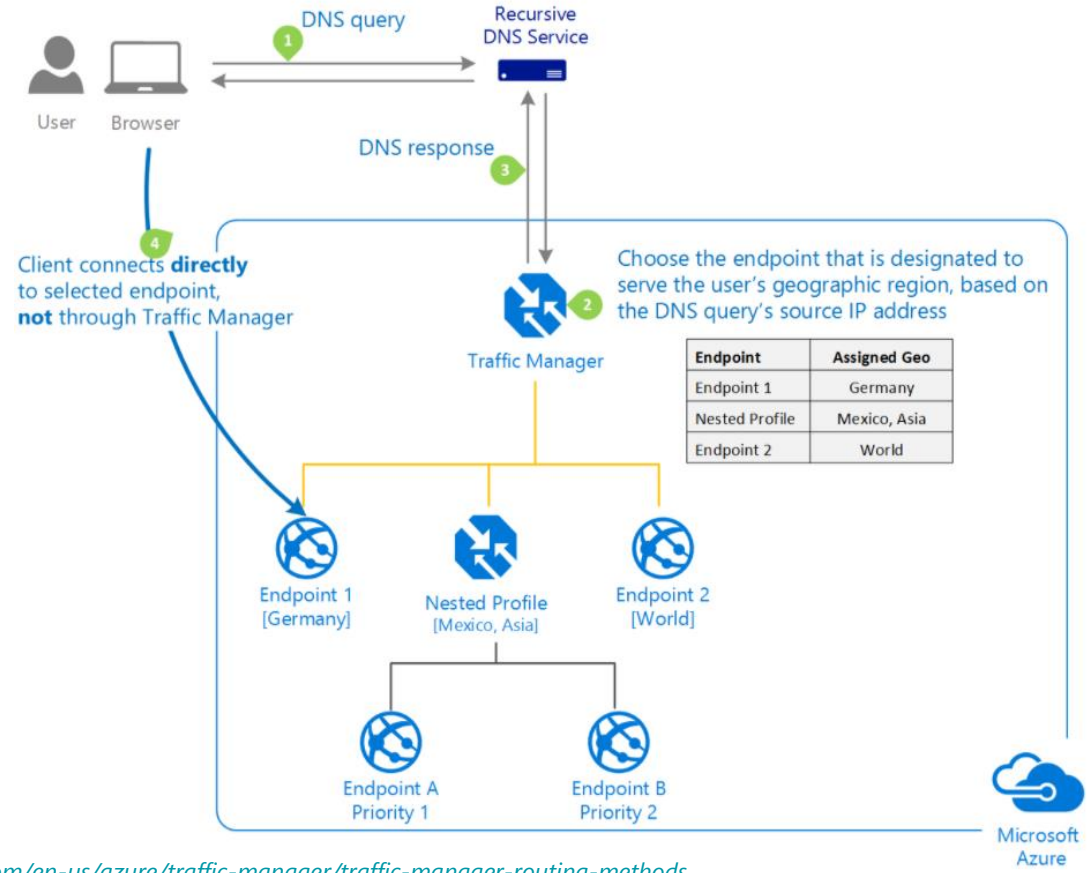


Source: https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods

Routing Method - Performance

- Traffic is routed to the endpoint nearest to the user
- Uses network latency to find nearest endpoint
- Maintains Internet Latency Table with round-trip time between a certain IP range and Azure datacenter location
- In case more users are coming from a location and diverted to the same endpoint, endpoint may become overloaded

Routing Method - Geographic



Source: https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods

Routing Method - Geographic

- Traffic from particular region/countries/states can be assigned to an endpoint
- One region can be mapped to one endpoint only
- If endpoint for a mapped region is not available, Traffic Manager returns NODATA response
- If no region is mapped for a request, Traffic Manager returns NODATA response

Routing Methods – Multivalue & Subnet

- Multivalue
  - Provides multiple endpoints to client in a single query response
  - Configure number of endpoints to return
  - Client can use any endpoint to connect
  - If one endpoint is down, client can connect to other endpoint
  - Only works for endpoints of External type
- Subnet
  - Allows to map specific set of end-user IP address ranges to endpoints
  - IP addresses in various endpoints should not conflict with each other
  - Define an endpoint with no IP address range as a fallback endpoint

Routing Methods

- Performance
- Priority
- Weighted
- Geographic
- Multivalue
- Subnet