



AZ-300T02

Module 03: Implementing Advanced Virtual Networking

Ahmad Majeed Zahoory



1

Module 03: Implementing Advanced Virtual Networking

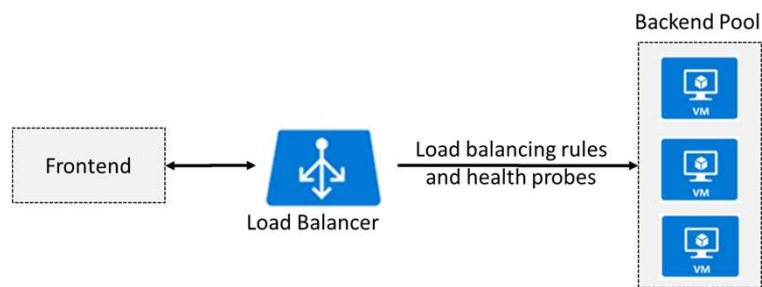
Lesson 01: Azure Load Balancer



2

Load Balancer

- Operates on OSI Layer 4 (TCP/UDP)
- Relies on health probes to determine status of backend pool
- Distributes traffic according to load balancing rules

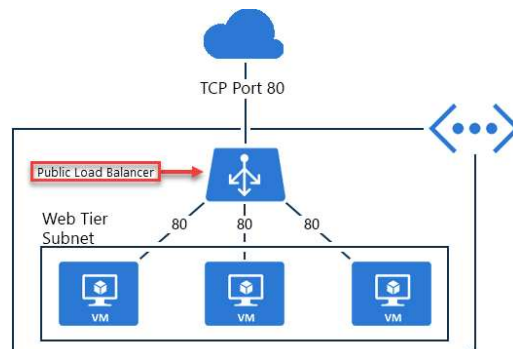


3

Public Load Balancer

Distributes traffic targeting a public IP address across backend VMs:

- **Frontend has one or more public IP addresses**
- **Backend VMs have private IP addresses**



4

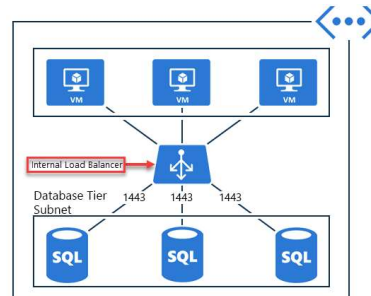
Internal Load Balancer

Distributes traffic targeting a private IP address across backend VMs:

- **Frontend has one or more private IP addresses**
- **Backend VMs have private IP addresses**

Supports load balancing:

- **Within a virtual network**
- **For a cross-premises virtual network**
- **For multi-tier applications**
- **For line-of-business applications**



5

Load Balancer SKUs

Two SKUs:

- **Basic**
- **Standard**



Constraints and considerations:

- **SKUs are not mutable.**
- **An Azure VM, Availability Set, or Azure VM Scale Set can reference one SKU, not both.**
- **A Load Balancer rule cannot span two virtual networks.**
- **There is no charge for the Basic load balancer.**
- **The Standard load balancer is charged based on number of rules and data processed.**

6

Backend Pool

Configuration depends on the load balancer SKU:

- **Standard:**
 - Up to 1,000 Azure VMs in the same virtual network, including VMs in availability sets and VM scale sets.
- **Basic:**
 - Up to 100 VMs in the same availability set or VM scale set.

SETTINGS

Backend pools

* Name: cesbackendpool

Associated to: Unassociated

Availability set

Single virtual machine

Virtual machine scale set



7

Load Balancer Rules

Determine traffic distribution

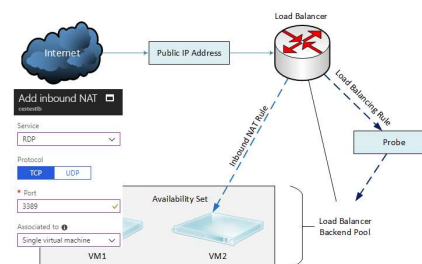
Require existing:

- **Frontend IP**
- **Backend pool**
- **Health probe**



Can be used with NAT rules:

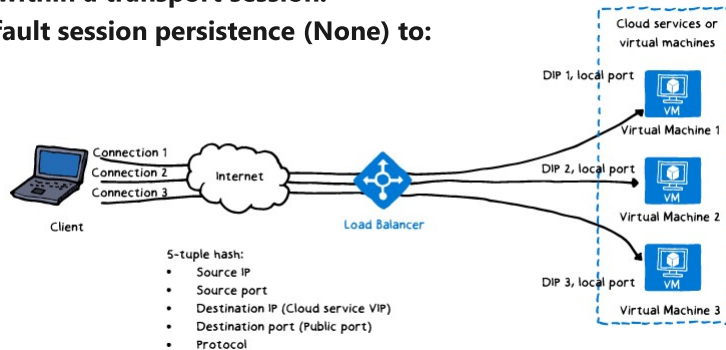
- **Allow connections to specific backend VMs**



8

Session Persistence

- Load balancing uses a hash to map traffic to backend pool VMs:
 - **5-tuple (source IP, source port, destination IP, destination port, and protocol type)**
 - **Stickiness applies only within a transport session.**
 - **You can change the default session persistence (None) to:**
 - **Client IP**
 - **Client IP and protocol**



9

Health Probes

Evaluate status of load balanced workloads:

- **Unhealthy threshold set to 2 consecutive failures (default)**
- **Interval set to 15 second (default)**

Support two protocols:

- **HTTP:**
 - **Expects HTTP 200 OK response**
- **TCP:**
 - **Tests for a successful TCP session**

10

Module 03: Implementing Advanced Virtual Networking

Lesson 02: Azure Application Gateway



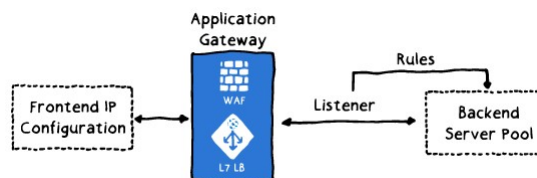
11

Application Gateway Components

Application Gateway is a load balancer operating on OSI Layer

Its components include:

- **Frontend IP configuration**
- **Backend server pool**
- **Listeners, including:**
 - front-end port
 - protocol (HTTP or HTTPS)
 - SSL certificate (optional).
- **Rules**
- **Web application firewall (WAF)**

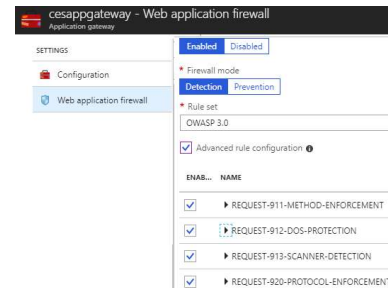
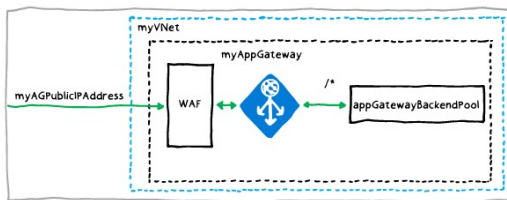


12

Web Application Firewall

Provides protection for backend server pool workloads:

- **Protects against common cyber threats (SQL injection, cross-side scripting, etc.)**
- **Uses OWASP rules**
- **Allows disabling rules that result in false positives**



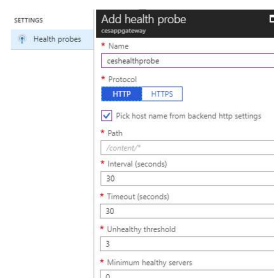
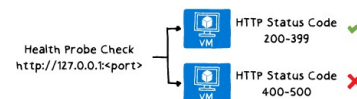
13

Health Probes

By default, health probes relies on healthy HTTP responses

Custom probes provide more control:

- **Facilitate more thorough health checks**
- **Support custom values of:**
 - Minimum healthy servers
 - Unhealthy threshold
 - Interval
 - Timeout
 - Path



14

Application Gateway Sizing

Application Gateway is available in 3 SKUs:

- **Small: intended for development and testing only**
- **Medium**
- **Large**

Average back-end page response size	Small	Medium	Large
6KB	7.5 Mbps	13 Mbps	50 Mbps
100KB	35 Mbps	100 Mbps	200 Mbps

Create application gateway

Name: cesappgateway

Tier: Standard (selected) WAF

SKU size: Medium

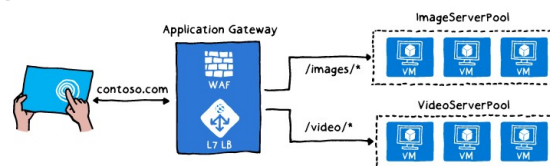
Instance count: 2

15

Path-Based Routing

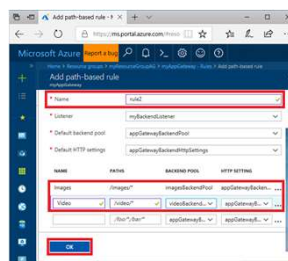
Directs traffic based on target URL, e.g.:

- **/images to one backend pool**
- **/video to another backend pool**



To implement:

- **Specify the path pattern, e.g.:**
 - **/images/* and /video/***



16

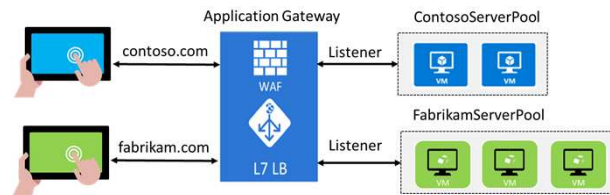
Multiple Site Hosting

Allows multiple web sites on the same Application Gateway instance:

- **Each with its own backend pool**
- **Up to the total of 20 web sites**

To implement:

- **Create 2 backend pools**
- **Create 2 listeners**
- **Create 2 routing rules**
- **Arrange the rules in the intended order**
 - Rules are processed in the order in which they are listed



17

Secure Sockets Layer Offload

Provides SSL termination at the gateway:

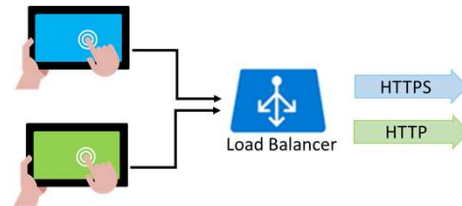
- **Eliminates performance impact of decryption on the backend pool VMs**
- **Requires uploading certificate and binding it to the appropriate listener**

18

Redirection and Session Affinity

Redirection:

- **Protocol redirection:**
 - Typically HTTP to HTTPS
- **Path-based redirection:**
 - Apply protocol redirection for specific path only:
 - e.g. /cart/*
- **Redirection to external sites**



Session affinity:

- **Cookie-based**
- **Directs traffic to the same backend pool VM**

19



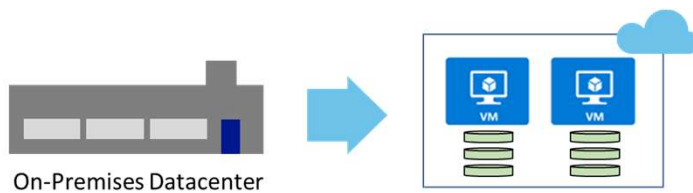
Lesson 03: VNet-to-VNet Connections



20

Site-to-Site Scenarios

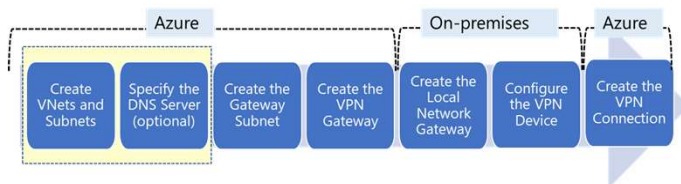
- Capacity On-Demand
- Strategic Migration
- Disaster Recovery



21

Implementing Site-to-Site VPN

1. Create VNets and subnets
2. Specify the DNS server (optional)
3. Create the Gateway subnet
4. Create the VPN Gateway
5. Create the Local Network Gateway
6. Configure the VPN device
7. Create the VPN Connection



22

Gateway Subnet

- Requires an IP range of /28 or larger
- Must be named GatewaySubnet
- Should not be associated to any Network Security Groups

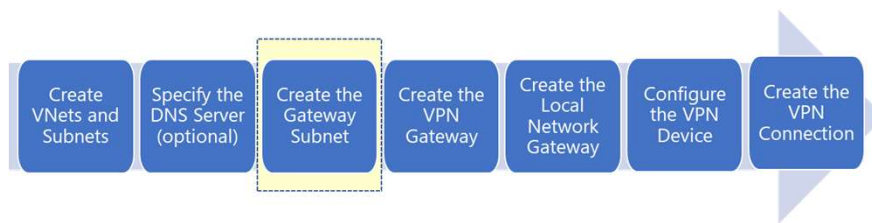
SETTINGS

+ Subnet + Gateway subnet

<> Subnets

search subnets

NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	SECURITY GROUP
default	10.1.0.0/24	251	-



23

Module 03: Implementing Advanced Virtual Networking

Lesson 04: ExpressRoute Connections



24

ExpressRoute

Private connection that extends on-premises network to:

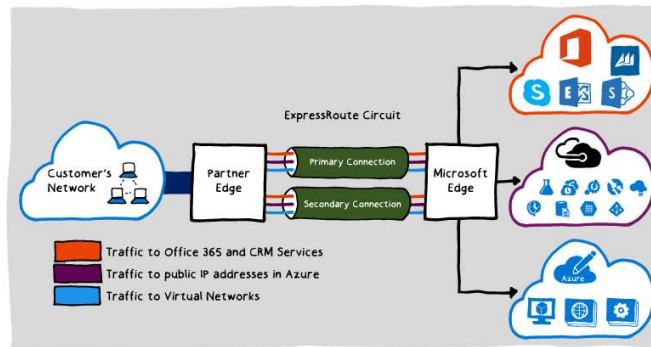
- **Microsoft Azure**
- **Office 365**
- **Dynamics 365**

Benefits:

- **Enhanced reliability**
- **Higher bandwidth**
- **Lower latency**
- **Increased security**

Common scenarios:

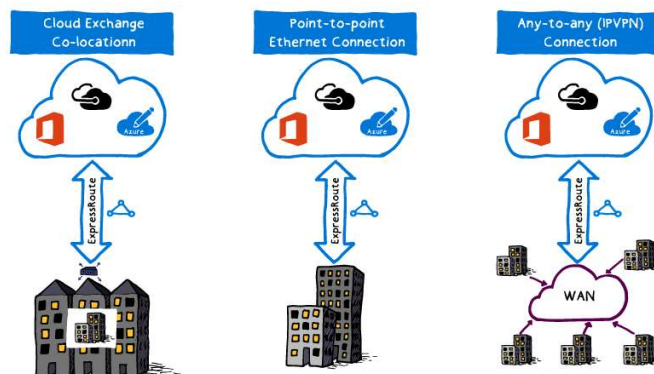
- **Data migration**
- **Business continuity**



25

ExpressRoute Connection Options

- **Cloud Exchange Co-location**
- **Point-to-point Ethernet Connection**
- **Any-to-any (IPVPN) Connection**



26

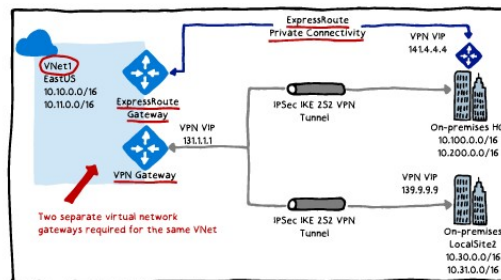
Site-to-Site and ExpressRoute Coexisting Connections

Configuration:

- VPN gateway and ExpressRoute gateway are deployed to the same GatewaySubnet

Benefits:

- **Extended scope of connectivity**
- **A cost effective failover**



27

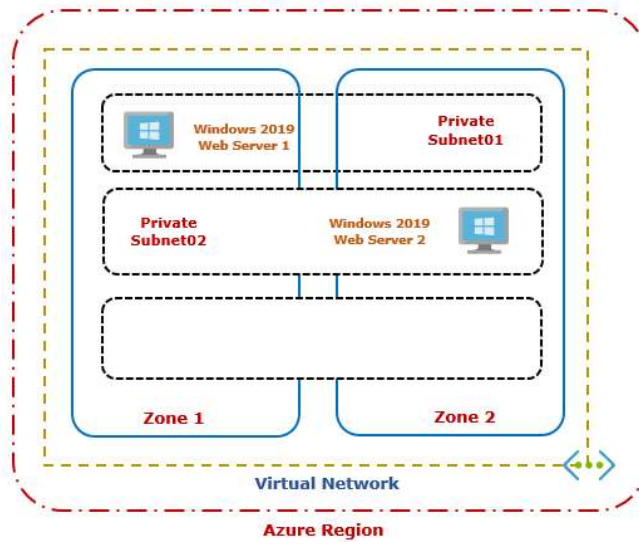
LAB [300TO02-M03-01]

1. Create Highly Available Secure Web Server.



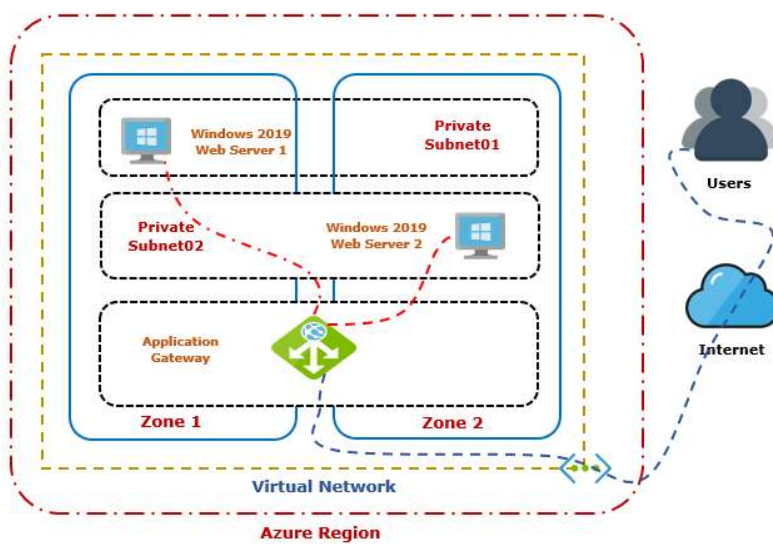
28

Part A



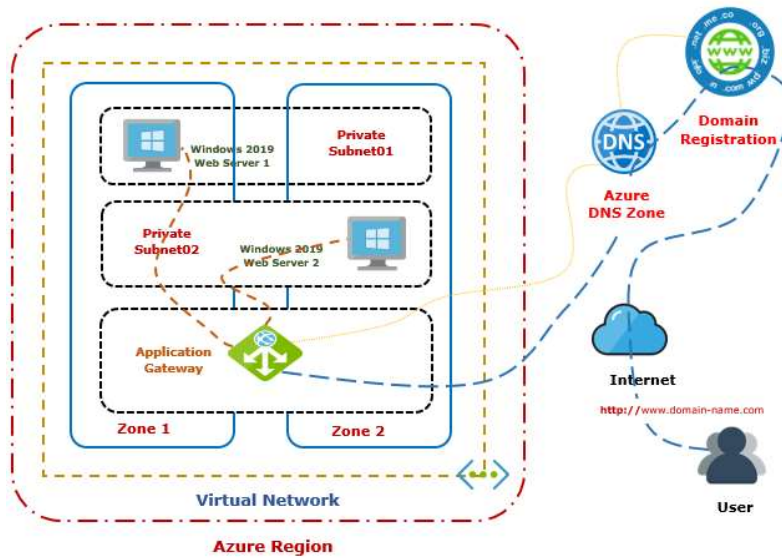
29

Part B



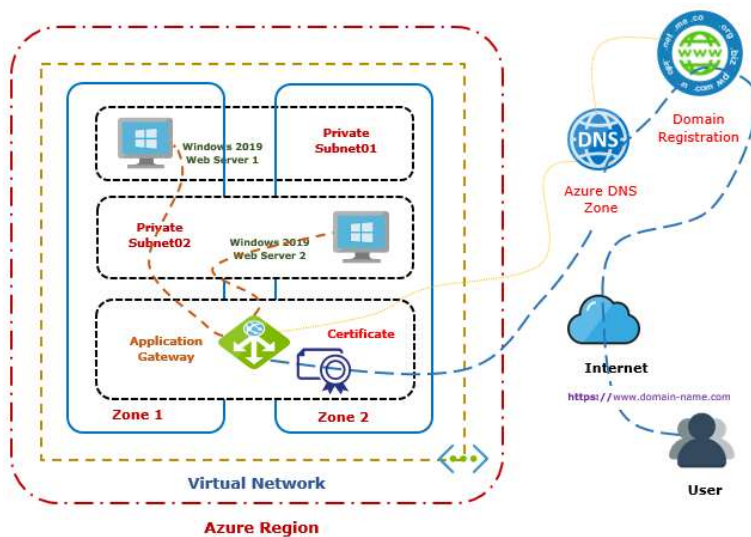
30

Part C



31

Part D



32

LAB [300TO02-M03-01]

1. Create Highly Available Secure Web Server.

a. **Services, Tools & Code used**

- i. Azure Virtual Machine
- ii. .Net Code
- iii. Application Gateway
- iv. Azure DNS Zone
- v. SSL Certificate

Duration: 40 mnts.



33



34