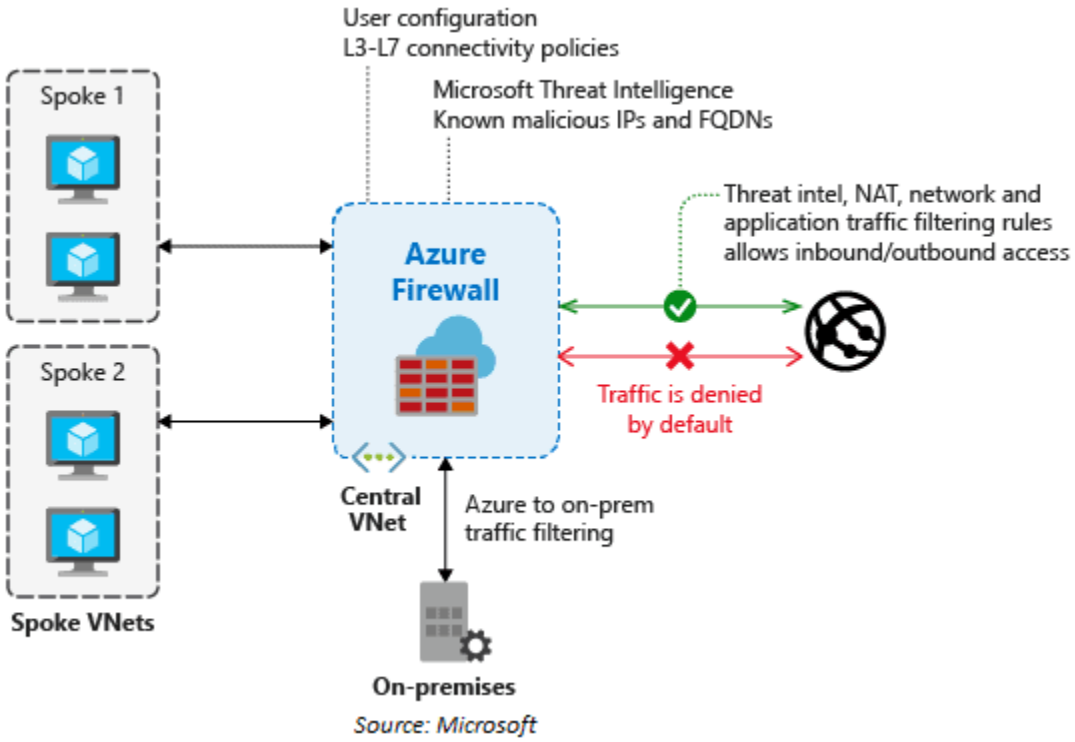
Implement Platform Protection

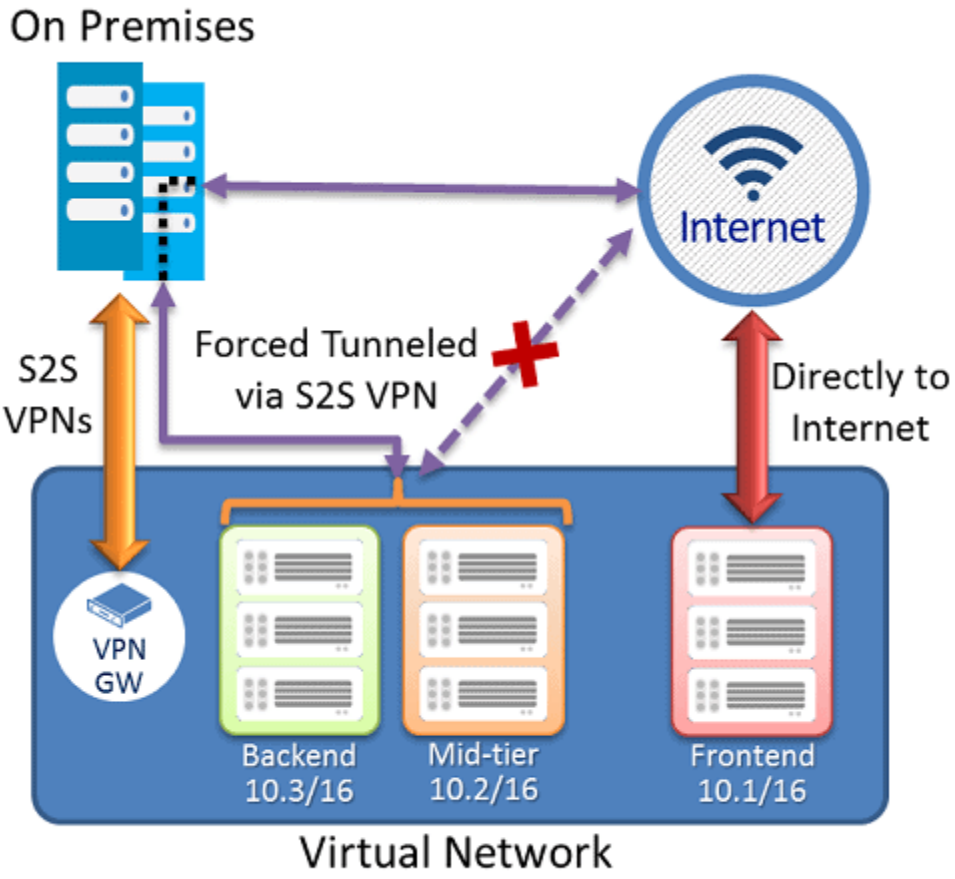
In this blog, I'll cover some **valuable insights**, including **Q&As** and **valuable links**, from Day 5 of our recent **Cloud Security for Azure, AWS, Google Cloud, and Oracle Live class**, where we discussed Firewall, Hub and Spock topology, Route table, Load balancer, NAT, Application gateway, WAF, CDN, and others.

Azure Firewall

Azure Firewall is a managed, cloud-based network security service that safeguards the resources of your Azure Virtual Network. It's a stateful firewall as a service with high availability and complete cloud scalability built-in.



Q1. What is forced tunnelling in Azure Firewall?
Ans. Instead of travelling directly to the Internet, you can route all Internet-bound traffic to a selected next-hop when configuring a new Azure Firewall. You must activate the Forced Tunnel configuration in Azure Firewall.

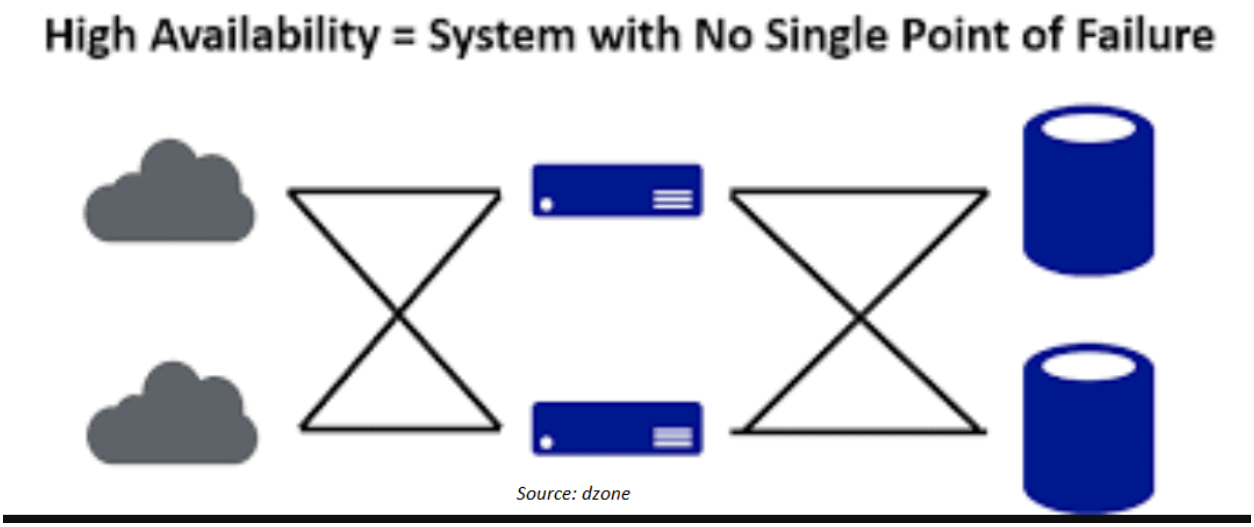


Source: Microsoft

For example, you may advertise a default route via BGP or use a User Defined Route (UDR) to force traffic to an on-premises edge firewall or other networks virtual appliance (NVA) to handle network traffic before it is sent to the Internet.

What do you mean by High Availability and Scalability?

High availability refers to the capacity of computing infrastructure to continue operating even if some of its components fail. This is vital for mission-critical systems that cannot tolerate service interruptions, and any downtime can result in damage or financial loss.



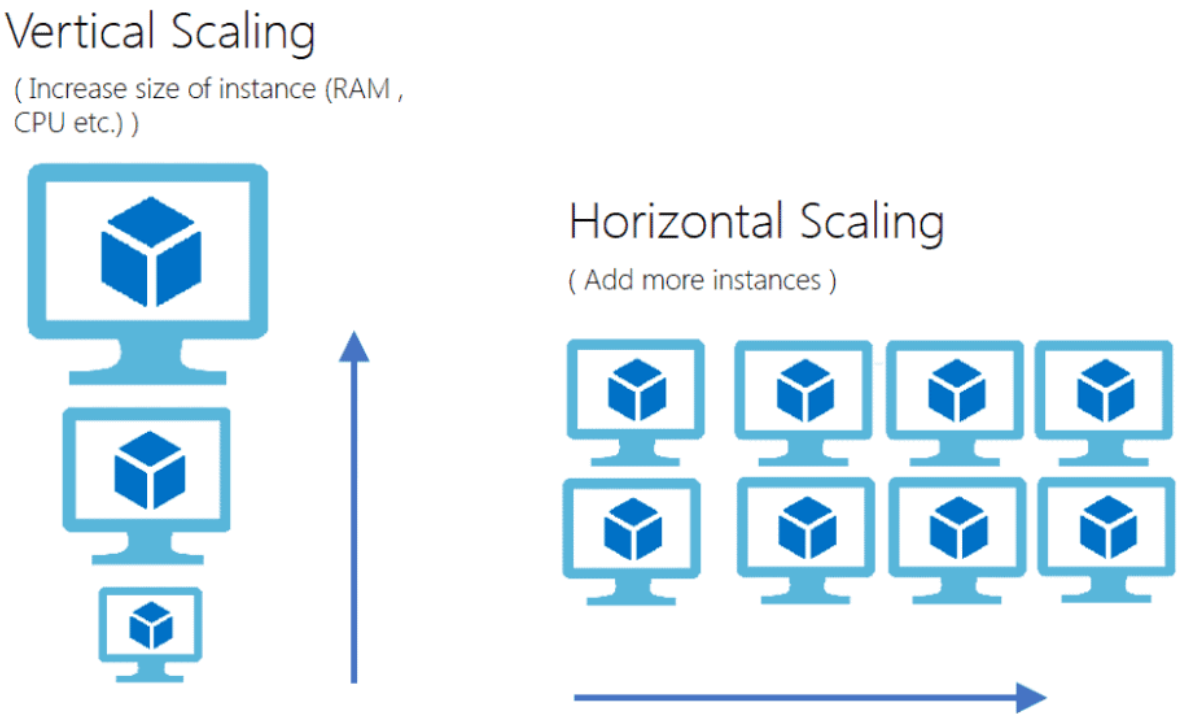
Highly available systems ensure a specific level of uptime—for example, a system with 99.9% uptime will be down only 0.1 percent of the time—0.365 days or 8.76 hours every year. The number "nine" is frequently used to represent a high level of availability. "Five nines," for example, denotes a system that is operational 99.999 percent of the time.

Q2. What is SLA?
Ans. It is Service-level agreements (SLAs) that describe Microsoft's commitments for uptime and connectivity.

Q3. What is planned and unplanned downtime?
Ans. Downtime can be divided into two categories. The goal of planned downtime is to make upgrades and configuration changes. In contrast, unplanned downtime is unavoidable owing to events such as systemwide failures and power outages.

Scalability

Scalability refers to a system's capacity to respond to changes in workload or traffic to a web application. One of the best aspects of the Azure service is its ability to scale automatically based on the application's needs.



Q4. What are some Azure Firewall concepts?
Ans: Azure Firewall supports rules and rule sets. A rule collection is a group of rules with the same priority and order. The rule collections are performed in the order in which they were created. All rules are terminating, and network rule collections have a higher priority than application rule collections.

There are three types of rule collections:

- *Application rules*: Configure fully qualified domain names (FQDNs) that can be accessed from a subnet.
- *Network rules*: Configure rules that contain source addresses, protocols, destination ports, and destination addresses.
- *NAT rules*: Configure DNAT rules to allow incoming Internet connections

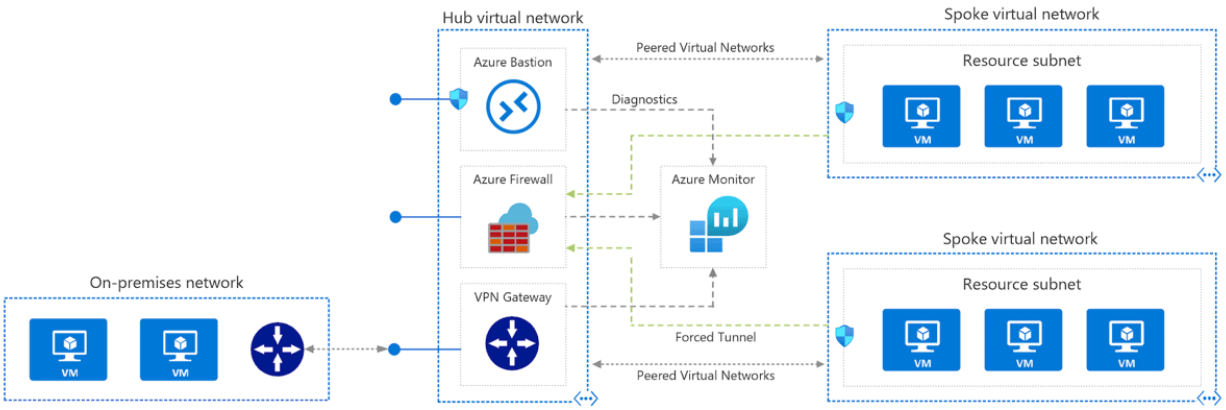
Q5. Does Azure Firewall support inbound traffic filtering?
Ans. Inbound and outbound filtering is supported by Azure Firewall. Non-HTTP/S protocols are often protected from inbound traffic. Protocols such as RDP, SSH, and FTP are examples. Use a web application firewall like Azure Web Application Firewall for the greatest inbound HTTP/S protection (WAF).

Q6. Is Network Security Groups (NSGs) supported on the AzureFirewallSubnet?

Ans. Azure Firewall is a managed service that provides various layers of protection, including platform protection via NIC level NSGs (not viewable). NSGs at the subnet level isn't required on the AzureFirewallSubnet, thus they're turned off to prevent service interruptions.

Hub and Spoke Topology

Many spoke virtual networks connect to the hub virtual network, which serves as a central point of connectivity. The hub can also serve as a point of connection for your on-premises networks. The spoke virtual networks can be utilised to separate workloads via peering with the hub. Cost reductions, overcoming subscription limits, and workload segregation are all advantages of employing a hub and spoke design.



Source: Microsoft

One **virtual network hub** and **two peer spokes** are included in this deployment. In addition, an **Azure Firewall** and an **Azure Bastion host** are installed. **Virtual computers** in the first spoke network and a **VPN gateway** are optional additions to the implementation.

Use cases

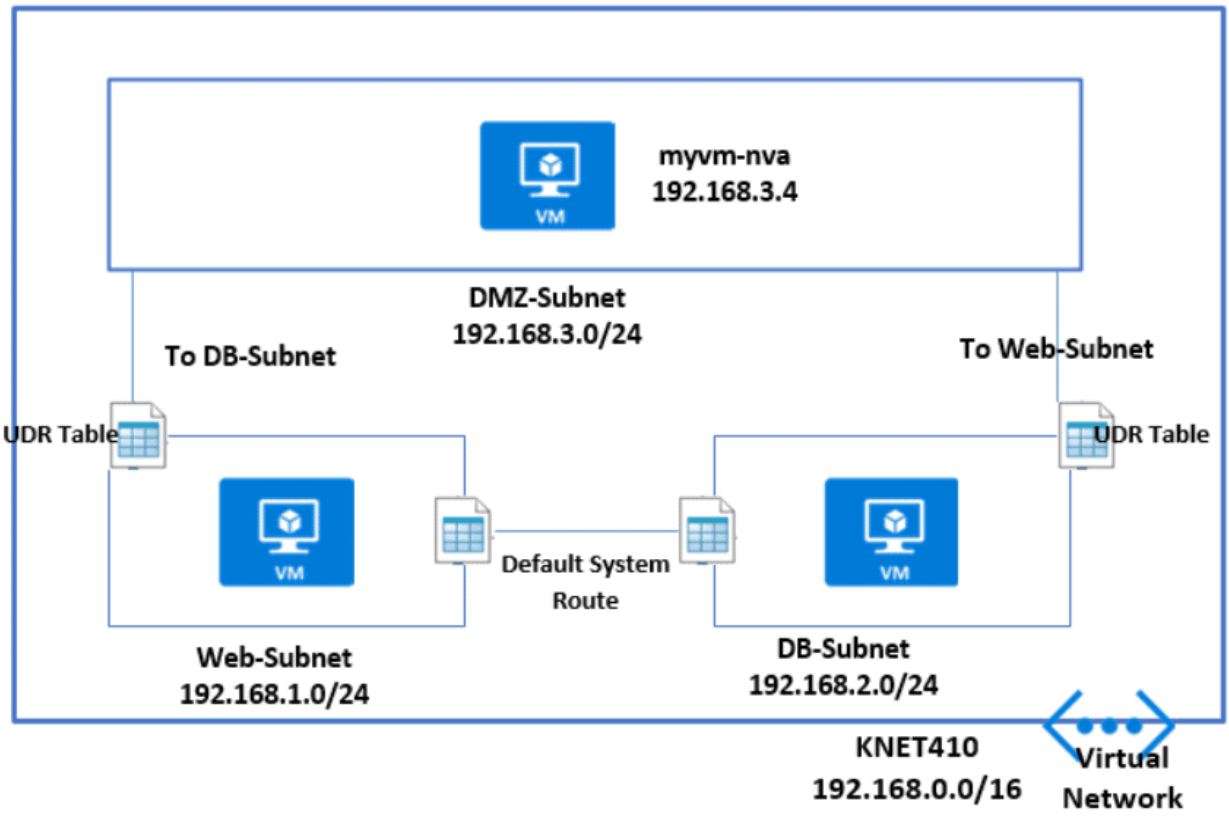
Typical uses for this architecture include:

- Workloads that require shared services such as DNS, IDS, NTP, or AD DS and are deployed in different environments such as development, testing, and production.
- Enterprises that demand centralised security control, such as a DMZ firewall in the hub and separated administration for each spoke's workloads.

Route table

You can use Azure Route Tables, also known as User Defined Routing, to build network routes so that your CloudGen Firewall VM can handle traffic between subnets and to the Internet. IP forwarding must be enabled on the network interfaces in order for them to receive and forward traffic.

User-defined routes are favoured over default system routes when different route types are present in a UDR route table. When there are numerous routes that lead to the same location, the more precise route is chosen.



Source: www.reddit.com

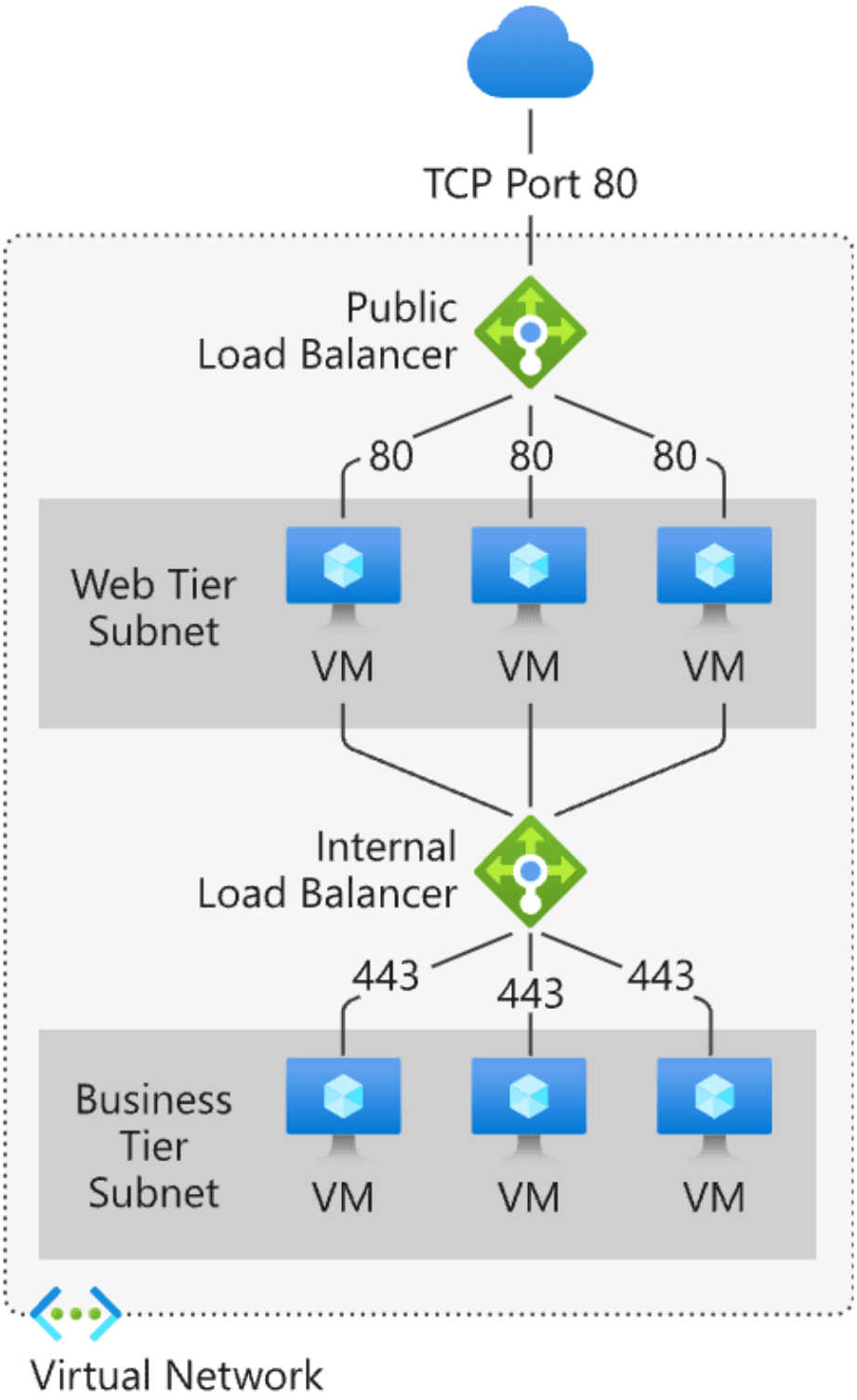
he following are possible with the default system routes that are always included in an Azure route table:

- Traffic within the virtual network
- Traffic to the Internet
- Traffic between different virtual networks using the Azure VPN Gateway
- Traffic from the virtual network to networks connected via the Azure VPN Gateway

Q7. A company wants to route their traffic to the internally provisioned network virtual appliance for compliance reasons. So, can we use Azure Route Table in that case to route traffic?
Ans: Yes, the company will use the Azure Route table to achieve the desired configuration.

Load balancer

Load balancing is the process of dispersing load (incoming network traffic) across a collection of backend resources or servers in an even manner. It is the client's single point of contact. Inbound flows that arrive at the load balancer's front end are distributed to backend pool instances by the load balancer. These flows are based on load-balancing rules and health probes that have been set up.



Source: Microsoft

[Recap] Day 5: Implement Platform Protection In Cloud Part – II

October 3, 2021 by Utkarsh Agarwal Agarwal Leave a Comment
135 views

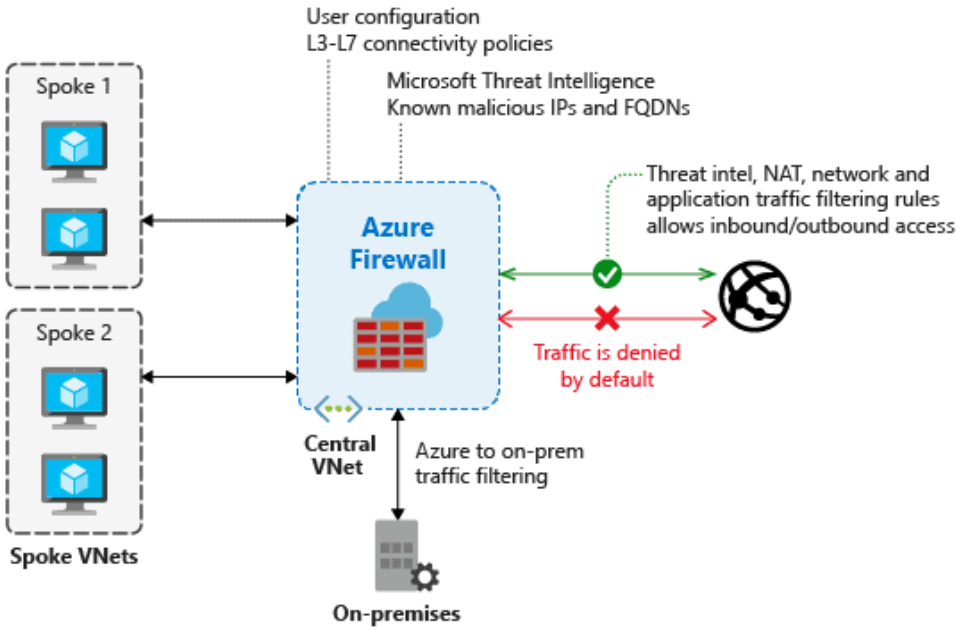
In this blog, I'll cover some **valuable insights**, including **Q&As** and **valuable links**, from Day 5 of our recen**t Cloud Security for Azure, AWS, Google Cloud, and Oracle Live class**, where we discussed Firewall, Hub and Spock topology, Route table, Load balancer, NAT, Application gateway, WAF, CDN, and others. We also did hands-on on Lab-8 & Lab-9 of our 18+ hands-on extensive labs in the live session.

On Day 4, we covered Bastion Host, VNet Peering, VPN gateway, and other topics in the previous week.

*So, here are **some of the Q&As** asked during the Live session from **Module 2: Implement Platform protection.***

Azure Firewall

Azure Firewall is a managed, cloud-based network security service that safeguards the resources of your Azure Virtual Network. It's a stateful firewall as a service with high availability and complete cloud scalability built-in.

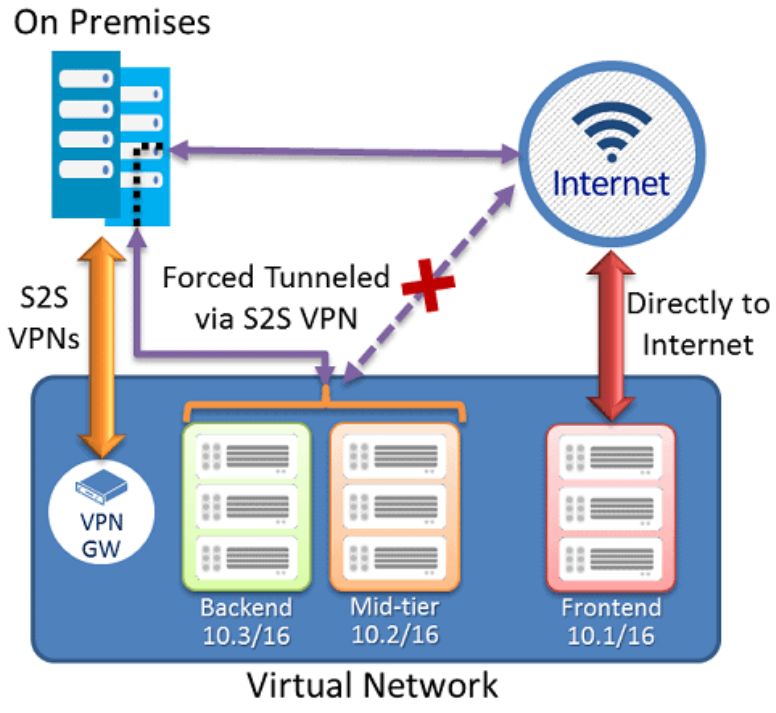


Source: Microsoft

>Know more about firewall

Q1. What is forced tunnelling in Azure Firewall?

Ans. Instead of travelling directly to the Internet, you can route all Internet-bound traffic to a selected next-hop when configuring a new Azure Firewall. You must activate the Forced Tunnel configuration in Azure Firewall.

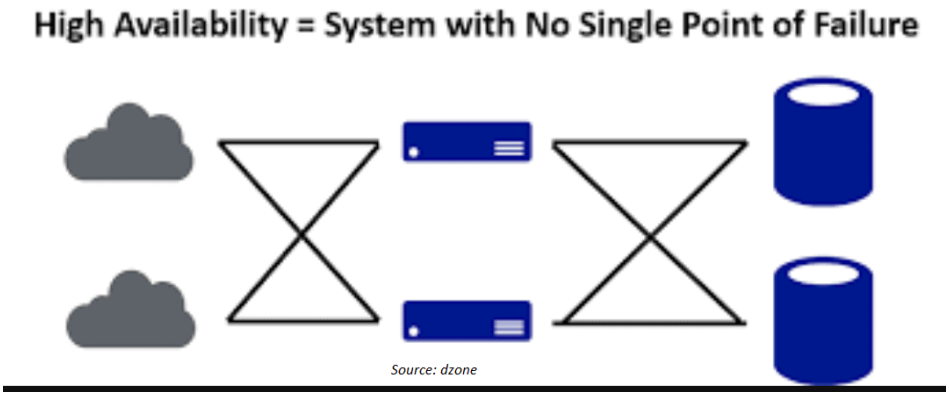


Source: Microsoft

For example, you may advertise a default route via BGP or use a User Defined Route (UDR) to force traffic to an on-premises edge firewall or other networks virtual appliance (NVA) to handle network traffic before it is sent to the Internet.

What do you mean by High Availability and Scalability?

High availability refers to the capacity of computing infrastructure to continue operating even if some of its components fail. This is vital for mission-critical systems that cannot tolerate service interruptions, and any downtime can result in damage or financial loss.



Highly available systems ensure a specific level of uptime—for example, a system with 99.9% uptime will be down only 0.1 percent of the time—0.365 days or 8.76 hours every year. The number “nine” is frequently used to represent a high level of availability. “Five nines,” for example, denotes a system that is operational 99.999 percent of the time.

>Know about Availability Set

Q2. What is SLA?

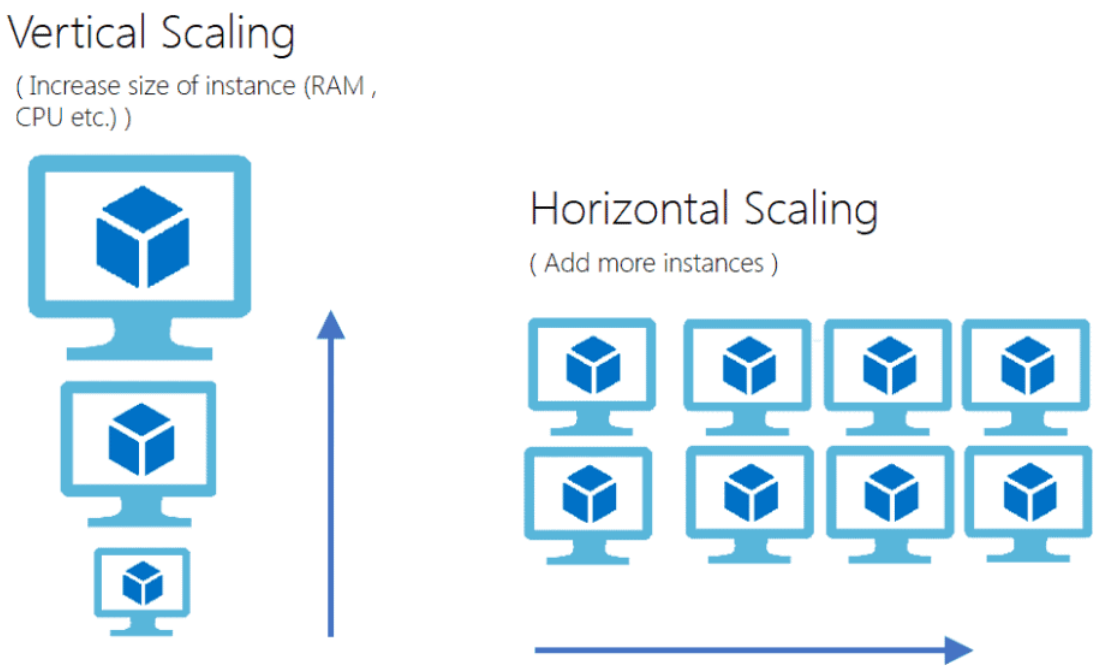
Ans. It is Service-level agreements (SLAs) that describe Microsoft’s commitments for uptime and connectivity.

Q3. What is planned and unplanned downtime?

Ans. Downtime can be divided into two categories. The goal of planned downtime is to make upgrades and configuration changes. In contrast, unplanned downtime is unavoidable owing to events such as systemwide failures and power outages.

Scalability

Scalability refers to a system’s capacity to respond to changes in workload or traffic to a web application. One of the best aspects of the Azure service is its ability to scale automatically based on the application’s needs.



>Know more about Scaling

Q4. What are some Azure Firewall concepts?

Ans: Azure Firewall supports rules and rule sets. A rule collection is a group of rules with the same priority and order. The rule collections are performed in the order in which they were created. All rules are terminating, and network rule collections have a higher priority than application rule collections.

There are three types of rule collections:

- *Application rules*: Configure fully qualified domain names (FQDNs) that can be accessed from a subnet.
- *Network rules*: Configure rules that contain source addresses, protocols, destination ports, and destination addresses.
- *NAT rules*: Configure DNAT rules to allow incoming Internet connections

Q5. Does Azure Firewall support inbound traffic filtering?

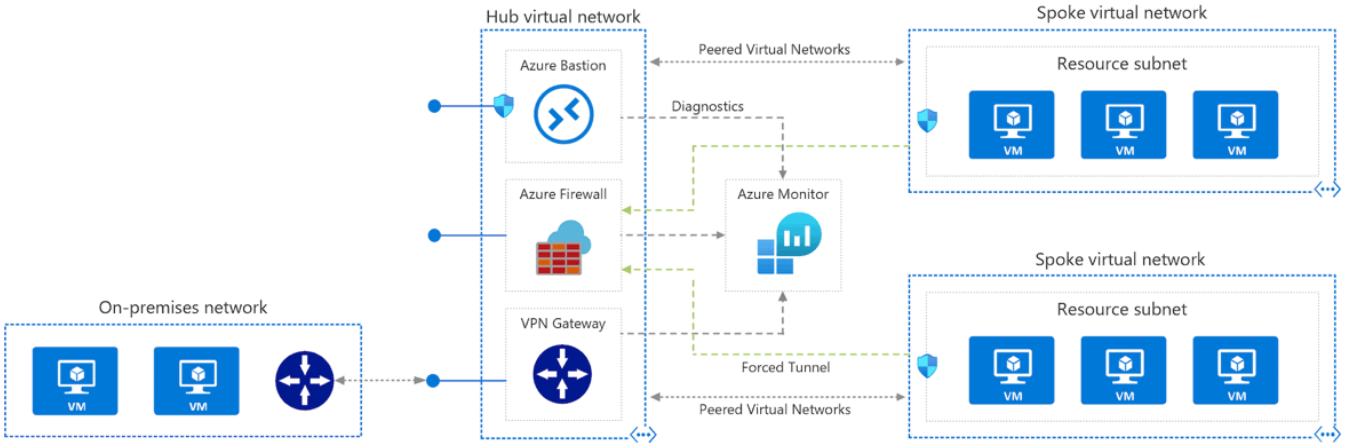
Ans. Inbound and outbound filtering is supported by Azure Firewall. Non-HTTP/S protocols are often protected from inbound traffic. Protocols such as RDP, SSH, and FTP are examples. Use a web application firewall like Azure Web Application Firewall for the greatest inbound HTTP/S protection (WAF).

Q6. Is Network Security Groups (NSGs) supported on the AzureFirewallSubnet?

Ans. Azure Firewall is a managed service that provides various layers of protection, including platform protection via NIC level NSGs (not viewable). NSGs at the subnet level isn't required on the AzureFirewallSubnet, thus they're turned off to prevent service interruptions.

Hub and Spoke Topology

Many spoke virtual networks connect to the hub virtual network, which serves as a central point of connectivity. The hub can also serve as a point of connection for your on-premises networks. The spoke virtual networks can be utilised to separate workloads via peering with the hub. Cost reductions, overcoming subscription limits, and workload segregation are all advantages of employing a hub and spoke design.



Source: Microsoft

One **virtual network hub** and **two peer spokes** are included in this deployment. In addition, an **Azure Firewall** and an **Azure Bastion host** are installed. **Virtual computers** in the first spoke network and a **VPN gateway** are optional additions to the implementation.

Use cases

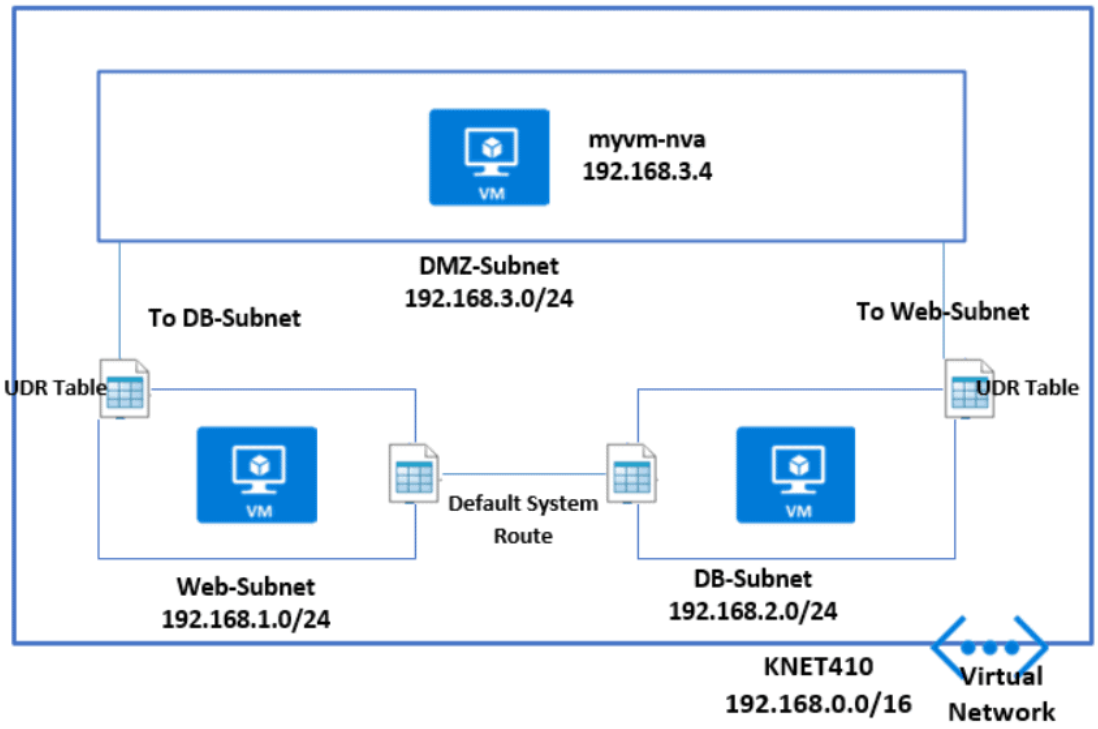
Typical uses for this architecture include:

- Workloads that require shared services such as DNS, IDS, NTP, or AD DS and are deployed in different environments such as development, testing, and production.
- Enterprises that demand centralised security control, such as a DMZ firewall in the hub and separated administration for each spoke's workloads.

Route table

You can use Azure Route Tables, also known as User Defined Routing, to build network routes so that your CloudGen Firewall VM can handle traffic between subnets and to the Internet. IP forwarding must be enabled on the network interfaces in order for them to receive and forward traffic.

User-defined routes are favoured over default system routes when different route types are present in a UDR route table. When there are numerous routes that lead to the same location, the more precise route is chosen.



Source: www.reddit.com

The following are possible with the default system routes that are always included in an Azure route table:

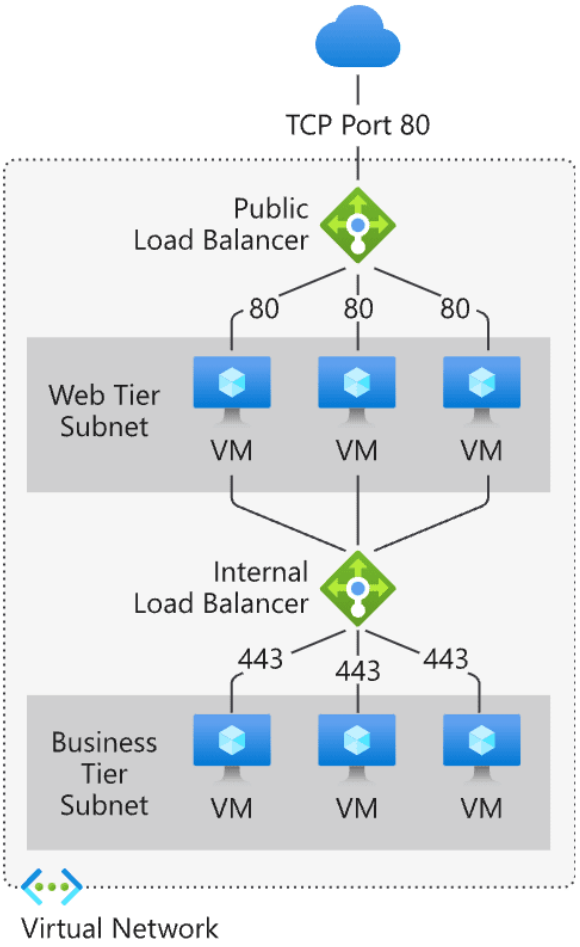
- Traffic within the virtual network
- Traffic to the Internet
- Traffic between different virtual networks using the Azure VPN Gateway
- Traffic from the virtual network to networks connected via the Azure VPN Gateway

Q7. A company wants to route their traffic to the internally provisioned network virtual appliance for compliance reasons. So, can we use Azure Route Table in that case to route traffic?

Ans: Yes, the company will use the Azure Route table to achieve the desired configuration.

Load balancer

Load balancing is the process of dispersing load (incoming network traffic) across a collection of backend resources or servers in an even manner. It is the client's single point of contact. Inbound flows that arrive at the load balancer's front end are distributed to backend pool instances by the load balancer. These flows are based on load-balancing rules and health probes that have been set up.



Source: Microsoft

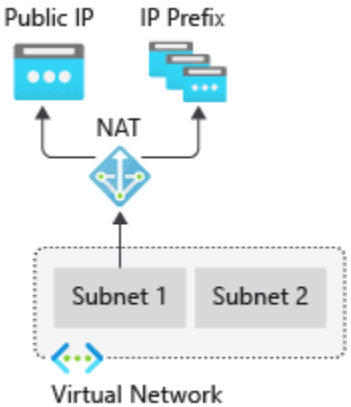
The nature of the IP address determines the type of load balancer created. Private IP address selection creates an internal load balancer. Public IP address selection creates a public load balancer.

	Public load balancer	Internal load balancer
Frontend IP configuration	Public IP address	Private IP address
Description	A public load balancer maps the public IP and port of incoming traffic to the private IP and port of the VM. Load balancer maps traffic the other way around for the response traffic from the VM. You can distribute specific types of traffic across multiple VMs or services by applying load-balancing rules. For example, you can spread the load of web request traffic across multiple web servers.	An internal load balancer distributes traffic to resources that are inside a virtual network. Azure restricts access to the frontend IP addresses of a virtual network that are load balanced. Front-end IP addresses and virtual networks are never directly exposed to an internet endpoint. Internal line-of-business applications run in Azure and are accessed from within Azure or from on-premises resources.
SKUs supported	Basic, Standard	Basic, Standard

Source: Microsoft

Virtual Network NAT

Virtual Network NAT (network address translation) facilitates virtual network outbound-only Internet communication. When a subnet is configured, all outward connectivity uses the static public IP addresses you choose.

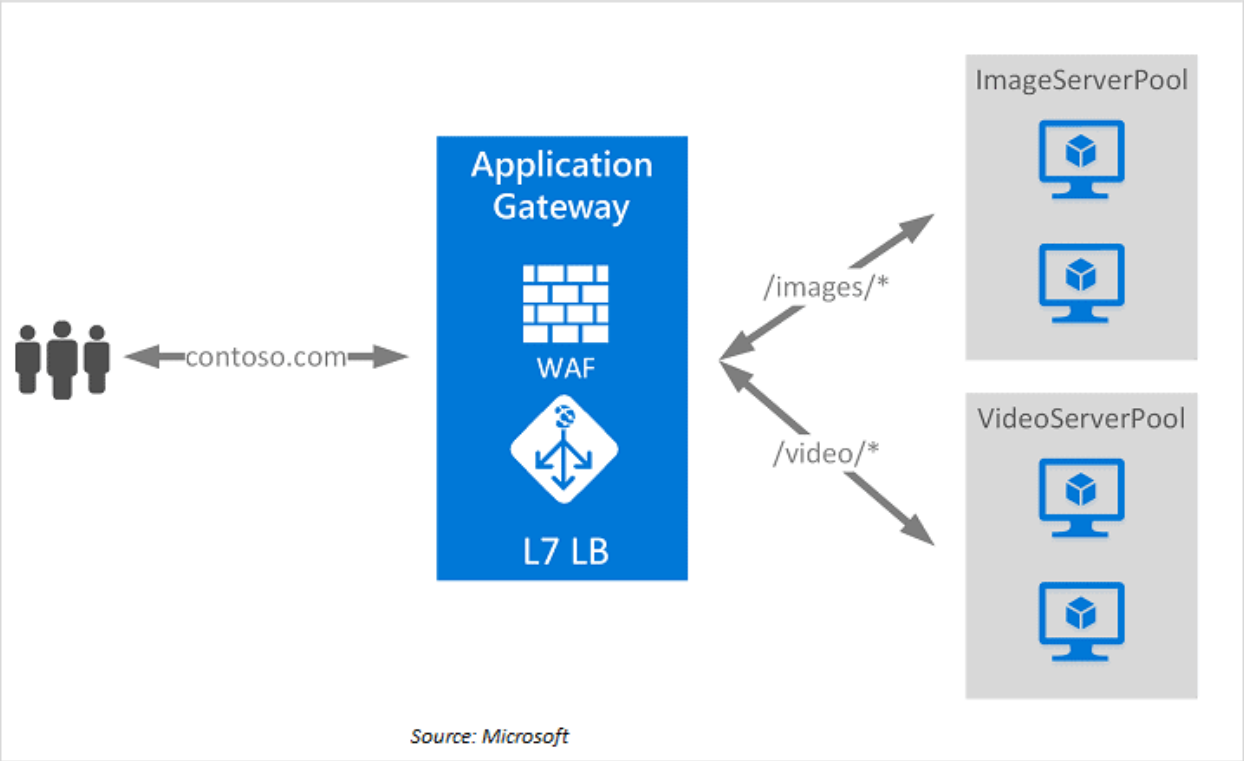


Source:Microsoft

Without a load balancer or public IP addresses directly tied to virtual machines, outbound communication is feasible. NAT is fully handled and extremely dependable.

Application Gateway

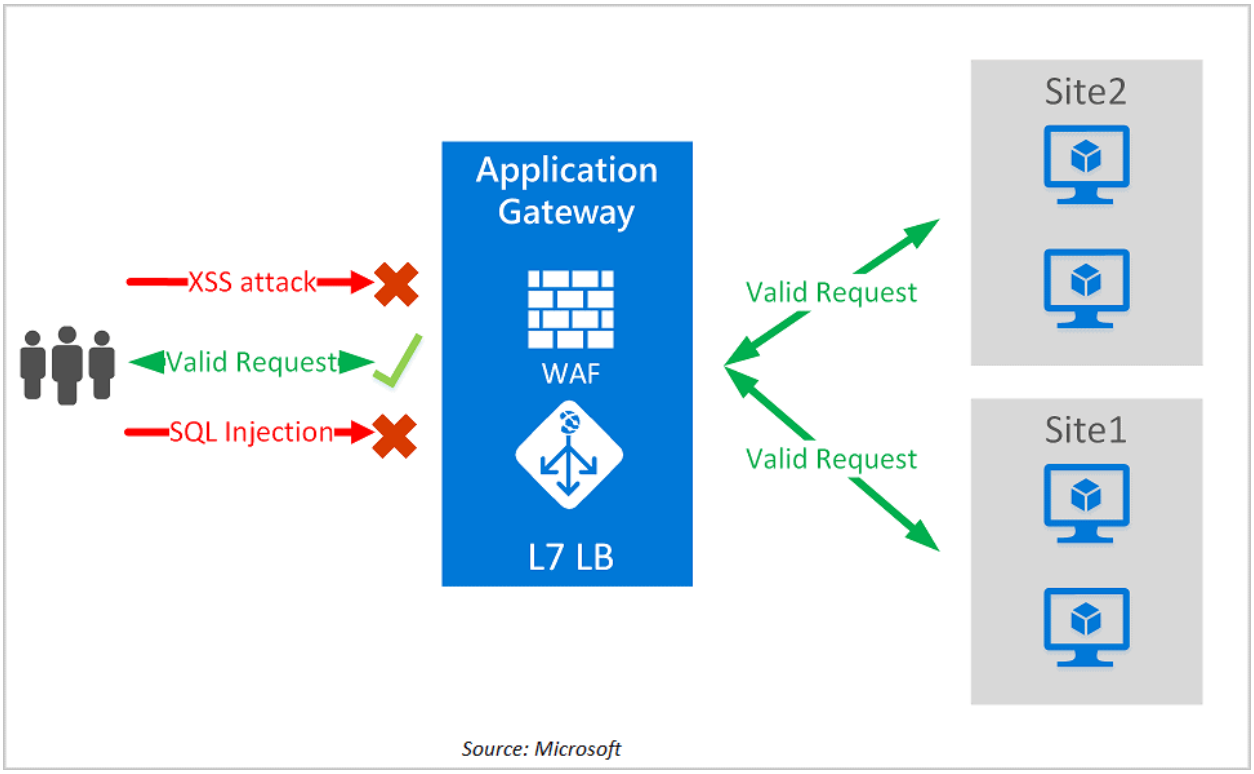
Azure Application Gateway is a web traffic load balancer that helps you manage web application traffic. Traditional load balancers route traffic based on source IP address and port to a destination IP address and port at the transport layer (OSI layer 4 – TCP and UDP).



Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example, URI path or host headers. For example, you can route traffic based on the incoming URL. So, if /images are in the incoming URL, you can route traffic to a specific set of servers (known as a pool) configured for images. If /video is in the URL, that traffic is routed to another pool that's optimized for videos.

Q8. How do Application Gateway and Azure Load Balancer differ?
Ans. Application Gateway is a layer 7 load balancer that solely handles web traffic (HTTP, HTTPS, WebSocket's, and HTTP/2). It has features like TLS termination, cookie-based session affinity, and round-robin traffic load balancing. At layer 4, the Load Balancer balances traffic (TCP or UDP).

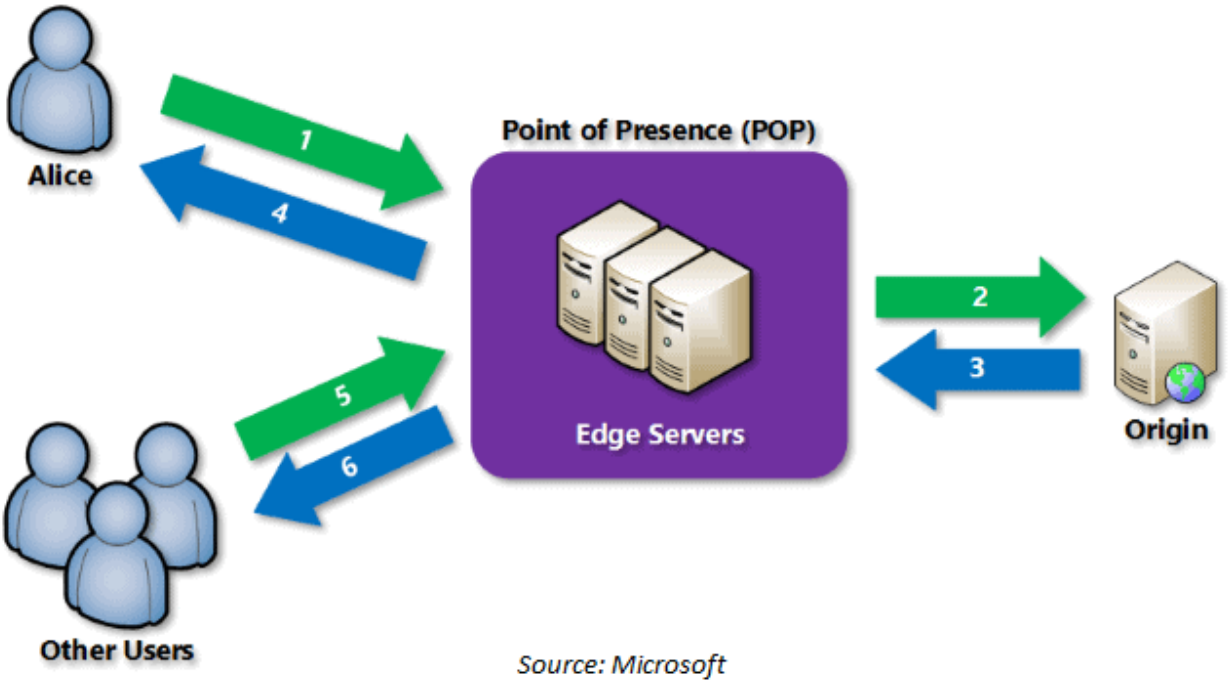
Q9. What is Azure Web Application Firewall on Azure Application Gateway?
Ans: The Azure Web Application Firewall (WAF) on Azure Application Gateway protects your web applications from common exploits and vulnerabilities in a centralized manner. Malicious attacks on web applications that make use of well-known flaws are becoming more widespread. Among the most popular attacks are SQL injection and cross-site scripting.



Source: Microsoft

CDN

The Azure Content Delivery Network (CDN) is a global CDN that allows you to send high-bandwidth content around the world. It might be hosted on Azure or anywhere else.



Source: Microsoft

Using the closest point of presence (POP) server, you can cache static assets loaded from Azure Blob storage, a web application, or any publicly available web server with Azure CDN. By exploiting numerous network and routing optimizations, Azure CDN can also accelerate dynamic content that cannot be cached.

Q10. Mention some of the advantages of CDN?
Ans. The following are some of the advantages of using Azure CDN to provide website assets:

- End users will benefit from enhanced performance and a better user experience, especially when utilising applications that require several round-trips to load content.
- Large scaling is used to better handle heavy loads that occur suddenly, such as at the commencement of a product launch event.
- User queries are distributed, and content is served directly from edge servers, resulting in less traffic being routed to the origin server.

Automation Account

Azure Automation is a cloud-based automation and configuration solution that allows you to manage your Azure and non-Azure environments in a consistent way. Process automation, configuration management, update management, shared capabilities, and heterogeneous features are all part of this solution. During the deployment, operations, and decommissioning of workloads and resources, automation offers you complete control.

Process Automation
Orchestrate processes using graphical, PowerShell, and Python runbooks

Configuration Management
Collect inventory
Track changes
Configure desired state

Update Management
Assess compliance
Schedule update installation

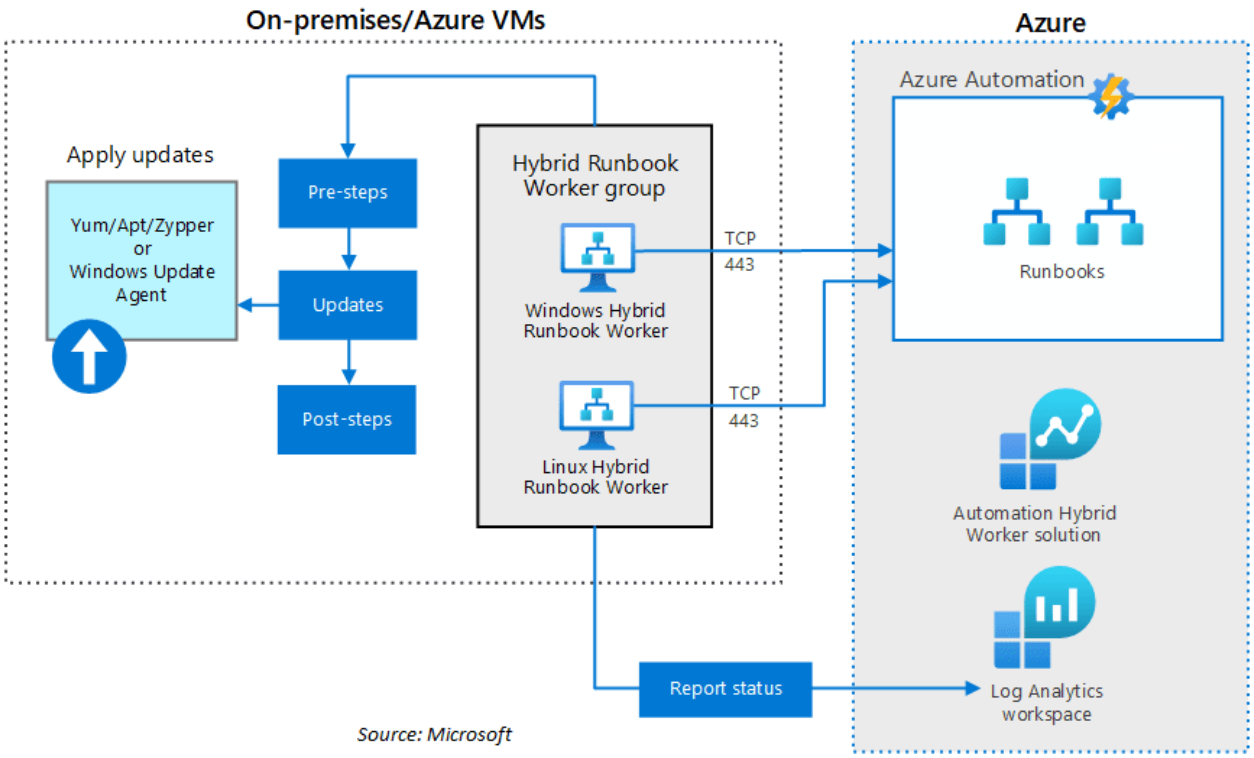
Shared capabilities
Role based access control
Secure, global store for variables, credentials, certificates, connections
Flexible scheduling
Shared modules
Source control support
Auditing
Tags

Heterogenous
Windows & Linux
Azure and on-premises

Source: Microsoft

Update Management

You can use Azure Automation's Update Management to manage operating system updates for your Windows and Linux virtual machines in Azure, as well as physical and virtual machines in on-premises environments and other cloud environments.

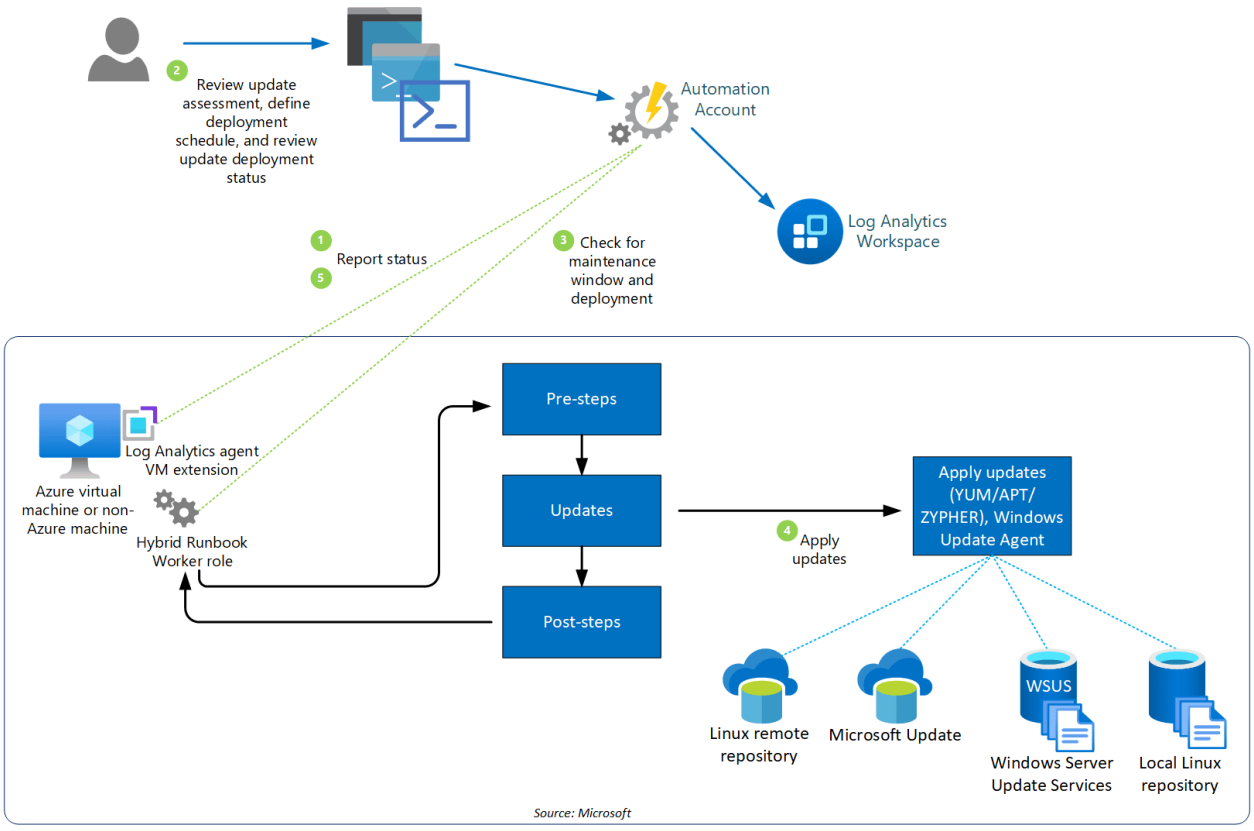


Source: Microsoft

You may have onboarded many customer tenants to Azure Lighthouse as a service provider. Update Management can be used to evaluate and schedule updates for computers in various subscriptions inside the same Azure Active Directory (Azure AD) tenant, or across tenancies using Azure Lighthouse.

Q10. What is Azure Lighthouse?
Ans. Azure Lighthouse allows multi-tenant management with increased scalability, automation, and resource governance.

Update Management reviews and applies security updates to all linked Windows Server and Linux servers, as shown in the diagram below.



Q.11 Can Update Management deploy updates across Azure tenants?
Ans. Yes, it can be deployed across azure tenants.