Caltech | Center for Technology & Management Education

Designing Infrastructure Solutions on Azure

Powered by simplilearn

Design a Network Solution

Learning Objectives

By the end of this lesson, you will be able to:

- Recommend a network architecture
- Recommend a solution for network addressing and name resolution
- Recommend a solution for network provisioning
- Recommend solutions for network security

Learning Objectives

By the end of this lesson, you will be able to:

- Recommend solutions for network connectivity
- Recommend solution for automating network management
- Recommend solution for load balancing and traffic routing

A Day in the Life of an Azure Architect

You are working as a principal engineer in an organization that is planning to migrate to the cloud and is looking for the below solutions:

- A solution that should enable the Azure resources' ability to securely connect with one another, the internet, and on-premises networks.
- A solution that can be utilized to deliver encrypted traffic over the public Internet between an Azure virtual network and an on-premises site.
- A solution that can be utilized to evenly distribute incoming network traffic across a collection of backend resources or servers.
- Your applications should be scalable, and you should be able to construct highly available services.

A Day in the Life of an Azure Architect

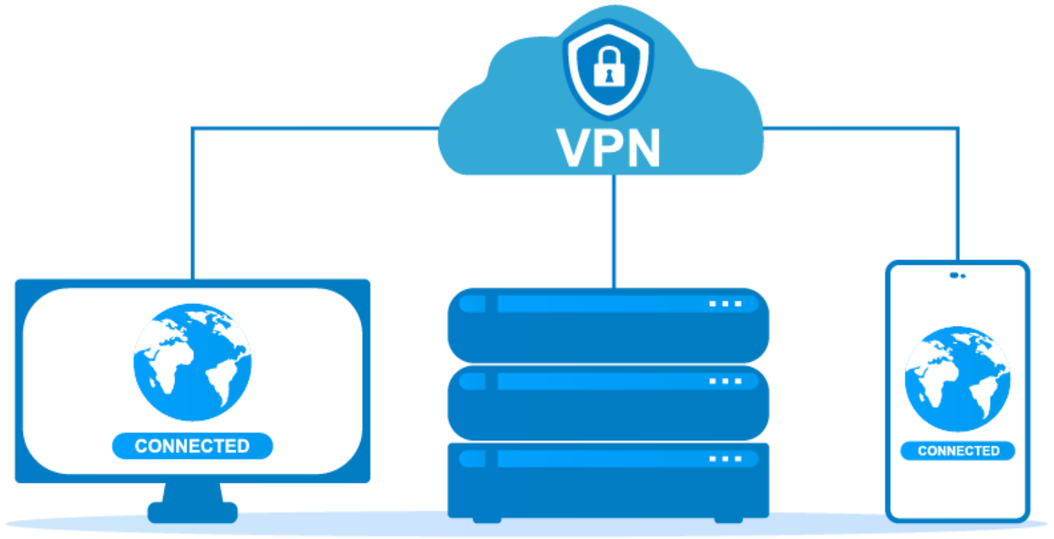
- Your company is also looking for different types of networking solutions which can be used to manage traffic to your web apps and may make routing decisions based on various types of attributes such as DNS name or URI path.
- A solution for building fast, secure, and broadly scalable online applications. This solution should be able to turn your worldwide consumer and enterprise apps into high-performing, tailored contemporary apps with content that reaches a global audience via Azure.

To achieve all of the above, along with some additional features, we would be learning a few concepts in this lesson that will help you find a solution for the above scenario.

Recommend a Network Architecture

Virtual Network

Virtual Network (VNet) is a logical representation of the network in the cloud.



VNets provide private connectivity between Azure Virtual Machines and other Azure services.

Virtual Network Concepts

Some of the Azure virtual network concepts are:

- Address space
- Subnet
- Region
- Subscription

When creating a VNet, the user must specify a custom private IP address space. By default, Azure assigns resources in a virtual network a private IP from the address space that users assign.

Virtual Network Concepts

Some of the Azure virtual network concepts are:

- Address space
- Subnet
- Region
- Subscription

A virtual network can be divided into one or more sub-networks and, these sub-networks are referred to as Subnets.

Virtual Network Concepts

Some of the Azure virtual network concepts are:

- Address space
- Subnet
- Region
- Subscription

While creating VNet, a single region or location for deployment can be selected.

Virtual Network Concepts

Some of the Azure virtual network concepts are:

- Address space
- Subnet
- Region
- Subscription

Virtual networks are scoped to a subscription.

Hub and Spoke Architecture

Hub-spoke topology can be explained as:

The hub virtual network acts as a central point of connectivity to many spoke virtual networks.

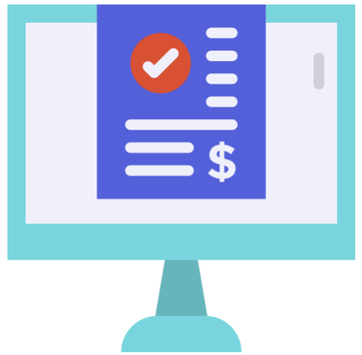
The hub can be used as the connectivity point for on-premises networks.

The spoke virtual networks peer with the hub and can be used to isolate workloads.

Hub and Spoke Architecture

Some of the benefits of Hub-spoke architecture are:

Cost savings

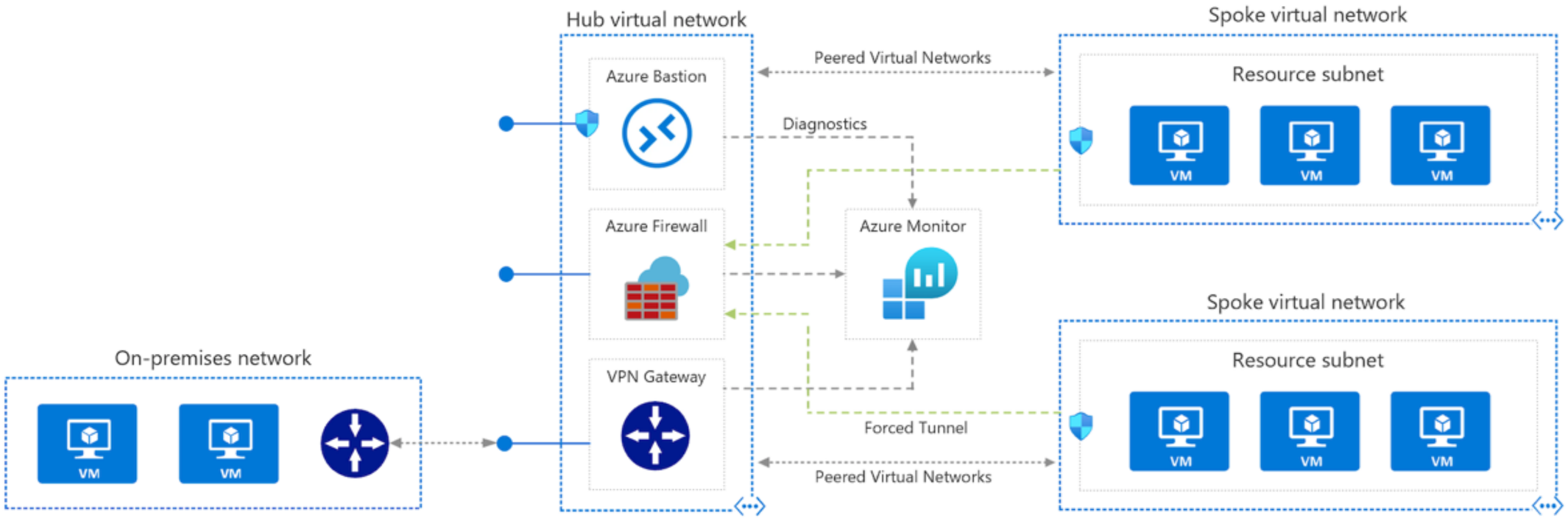


Overcoming subscription limit

Workload isolation

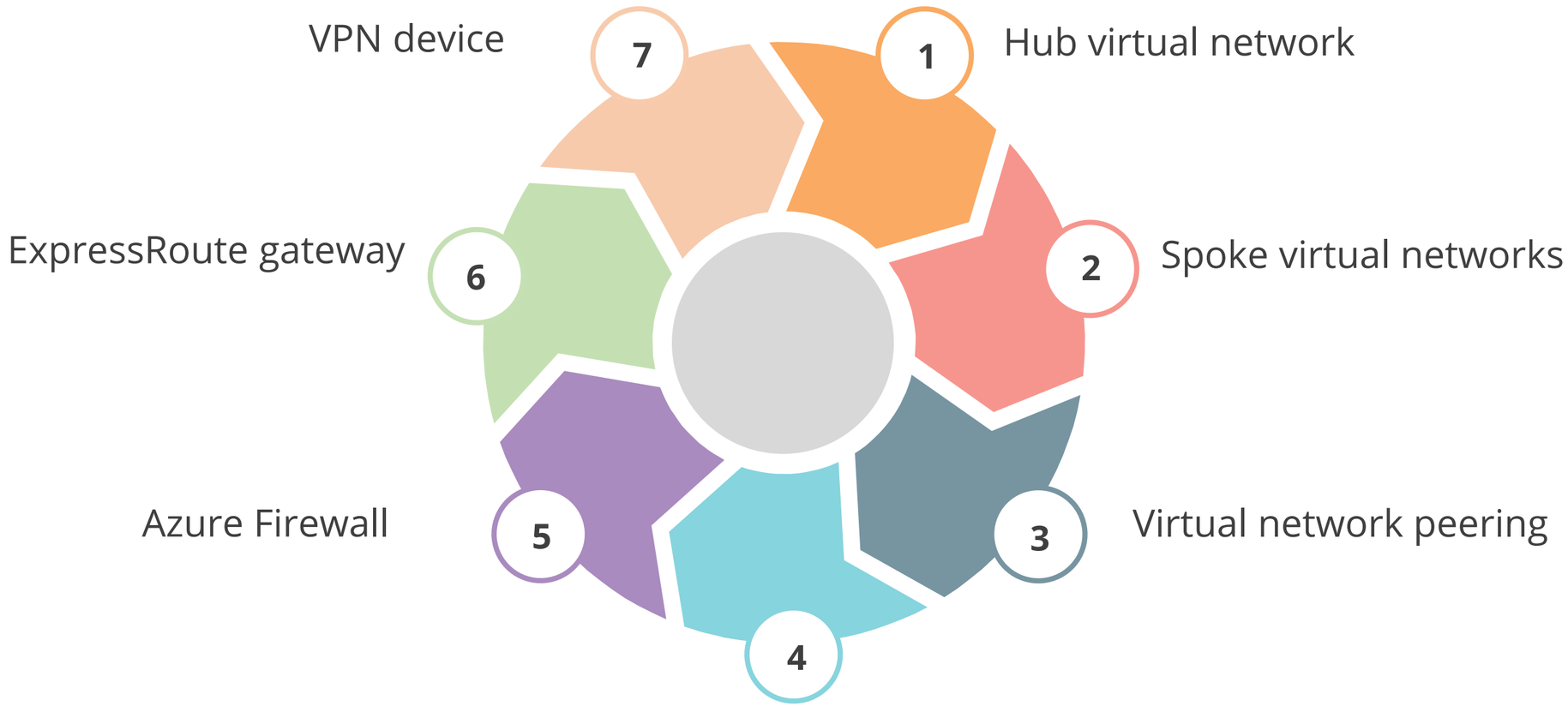
Hub and Spoke Architecture

Hub-spoke architecture is shown below:

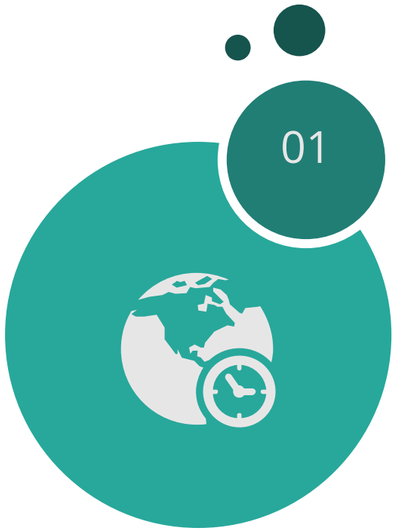


Components of Hub and Spoke Architecture

Hub-spoke architecture consists of the components below:



Use Cases of Hub and Spoke Architecture



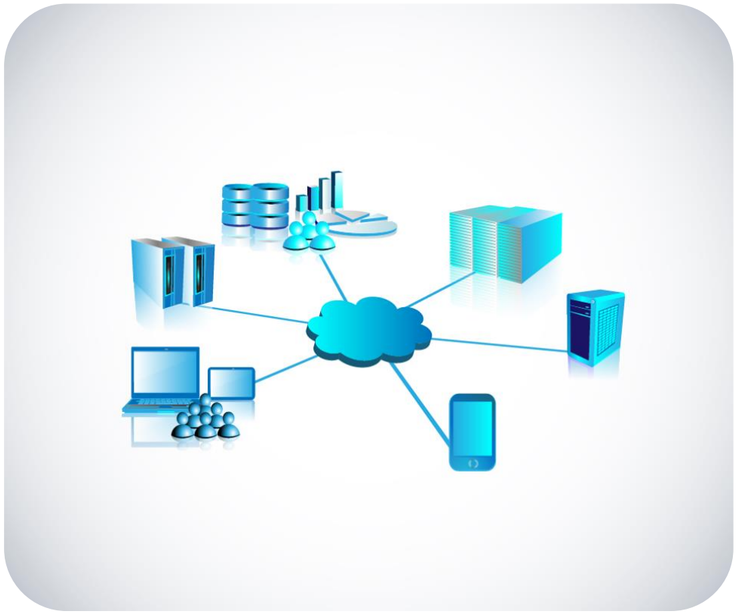
Workloads that require shared services are placed in the hub virtual network, while each environment is deployed to a spoke.

Workloads that require access to shared services but do not require connectivity to each other.

Enterprises that require central control and segregated management for the workloads in each spoke.

Hub-Spoke Network Topology with Virtual WAN

Hub-spoke topology with virtual WAN consists of:

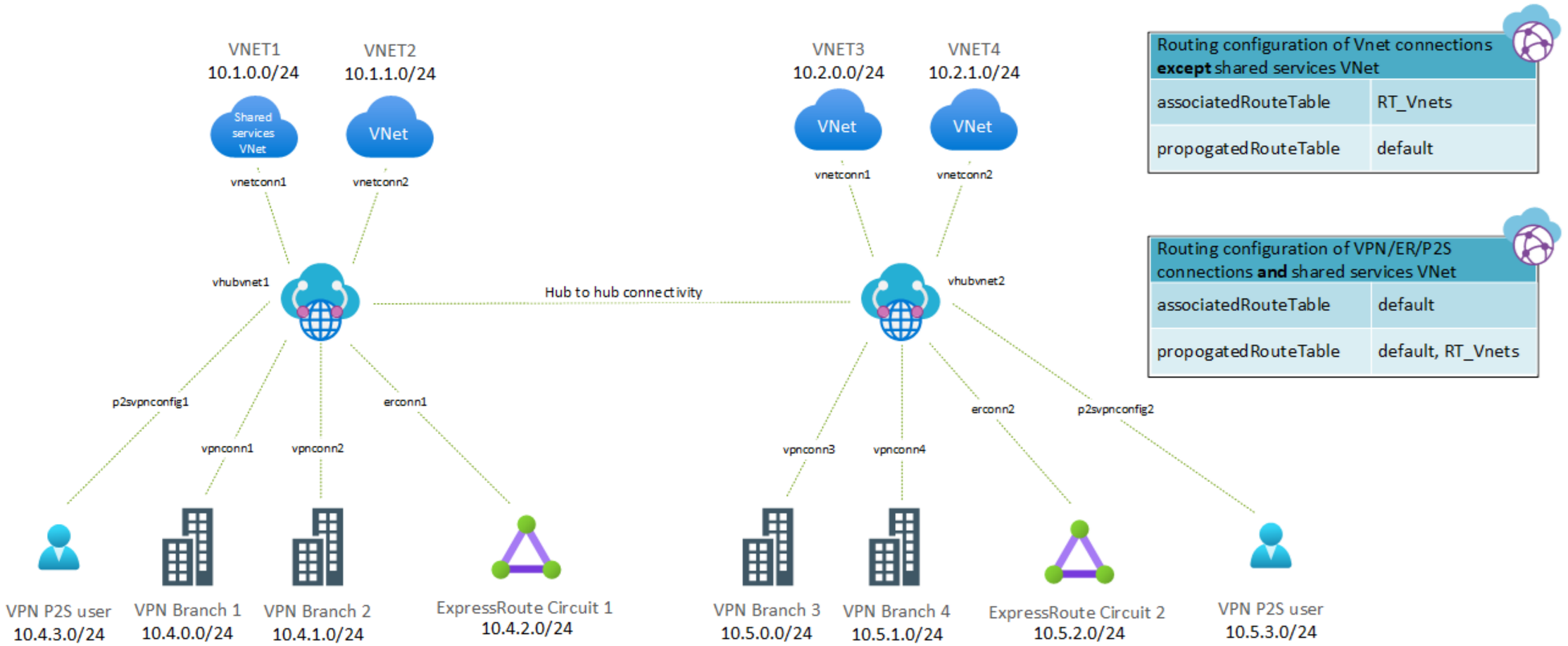


- Hub VNet is a connection point for several spoke VNets.
- Spoke VNets can be used to separate workloads via peering with the hub.
- Traffic travels between the on-premises data center(s) and the hub using an ExpressRoute or VPN gateway.

This approach makes use of Azure Virtual WAN (VWAN) to replace hubs as a managed service.

Hub-Spoke Network Topology with Virtual WAN

Hub-spoke topology with virtual WAN is shown below:



Routing configuration of Vnet connections **except** shared services VNet	
associatedRouteTable	RT_Vnets
propogatedRouteTable	default

Routing configuration of VPN/ER/P2S connections **and** shared services VNet	
associatedRouteTable	default
propogatedRouteTable	default, RT_Vnets

Components of Hub-Spoke Network Topology with Virtual WAN

Hub-spoke topology with virtual WAN architecture consists of the components below:

- On-premises network
- VPN device
- VPN or ExpressRoute gateway
- Virtual WAN hub
- Secured virtual hub
- Gateway subnet
- Spoke virtual networks
- Virtual network peering

Benefits of Hub-Spoke Network Topology with Virtual WAN

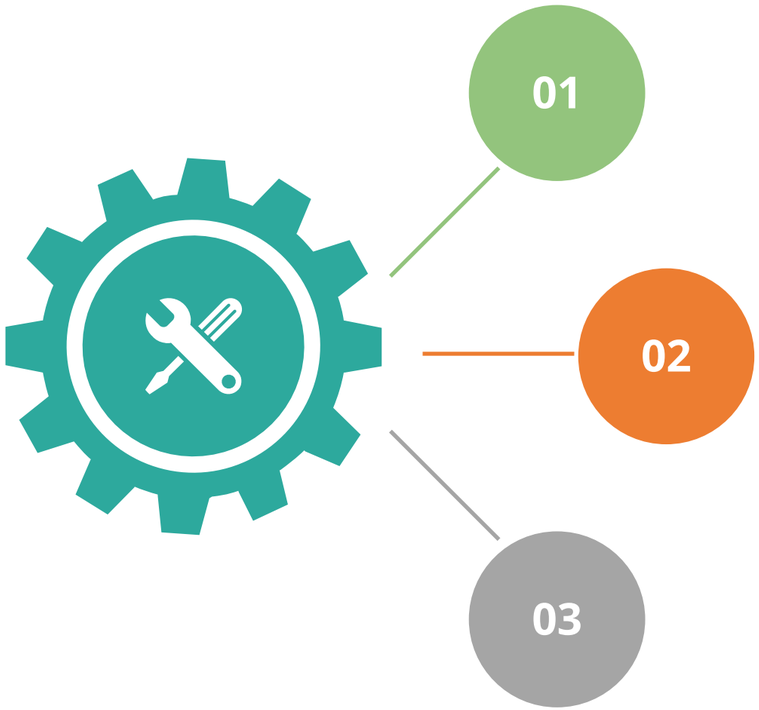
Some additional benefits of Hub-spoke architecture with virtual WAN are:

- Less operational overhead
- Cost savings
- Improved security
- Separation of concerns between central IT and workloads

Recommend a Solution for Network Addressing and Name Resolution

Name Resolution for Resources in Azure Virtual Networks

When resources deployed in virtual networks need to resolve domain names to internal IP addresses, they can use one of the three methods:



Azure DNS private zones

Azure-provided name resolution

Name resolution that uses DNS server

Name Resolution for Resources in Azure Virtual Networks

The table below shows the name resolution depending on different scenarios:

Scenario	Solution	DNS Suffix
Between VMs in the same VNet, Azure Cloud Services role instances	Azure DNS private zone, Azure-provided name resolution	Hostname or FQDN (Fully Qualified Domain Name)
Between VMs in different VNet or instances in different cloud services	Azure DNS private zones, Customer-managed DNS forwarding to Azure (DNS Proxy)	Hostname or FQDN
From App Service (Web App, Function or Bot) using VNet integration to VM in the same VNet	Customer-managed DNS forwarding to Azure (DNS Proxy)	FQDN only
From App Service Web App to VMs in the same VNet	Customer-managed DNS forwarding to Azure (DNS Proxy)	FQDN only
App Service Web app to VM in different VNet	Customer-managed DNS forwarding to Azure (DNS Proxy)	FQDN only

Name Resolution for Resources in Azure Virtual Networks

The table below shows the name resolution depending on different scenarios:

Scenario	Solution	DNS Suffix
On-premises computer and service name from VMs or role instances in Azure	Customer-managed DNS	FQDN only
Azure hostnames from on-premises computers	Forward queries to a customer-managed DNS proxy server in the corresponding VNet	FQDN only
Reverse DNS for internal IP	Azure DNS private zones, Azure-provided name resolution, or customer own DNS	Not applicable
Between VMs in different cloud services, not in virtual networks	Not supported	Not supported

Azure-Provided Name Resolution

Azure-provided name resolution provides basic authoritative DNS capabilities.

- Provides Azure DNS private zones or customer-managed DNS servers for full-featured DNS
- Supports internal name resolution for VMs and role instances in the same virtual network or cloud service

VMs and instances in a cloud service share the same DNS suffix, so the hostname alone is sufficient.

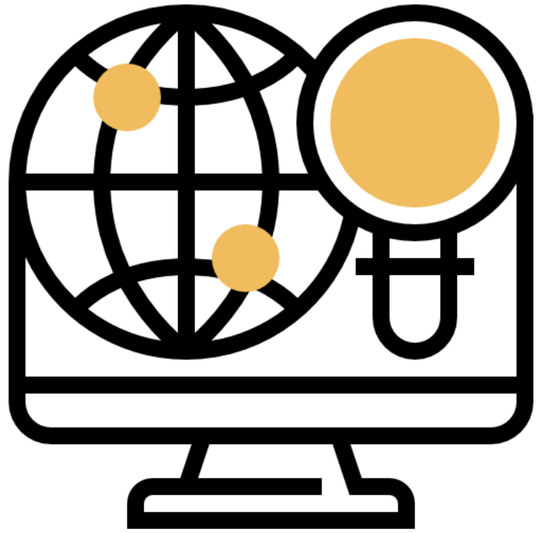
Azure-Provided Name Resolution

The DNS suffix is consistent across all virtual machines within a virtual network for virtual networks deployed using the ARM deployment model.

- FQDN is not needed
- DNS names can be assigned to both VMs and network interfaces

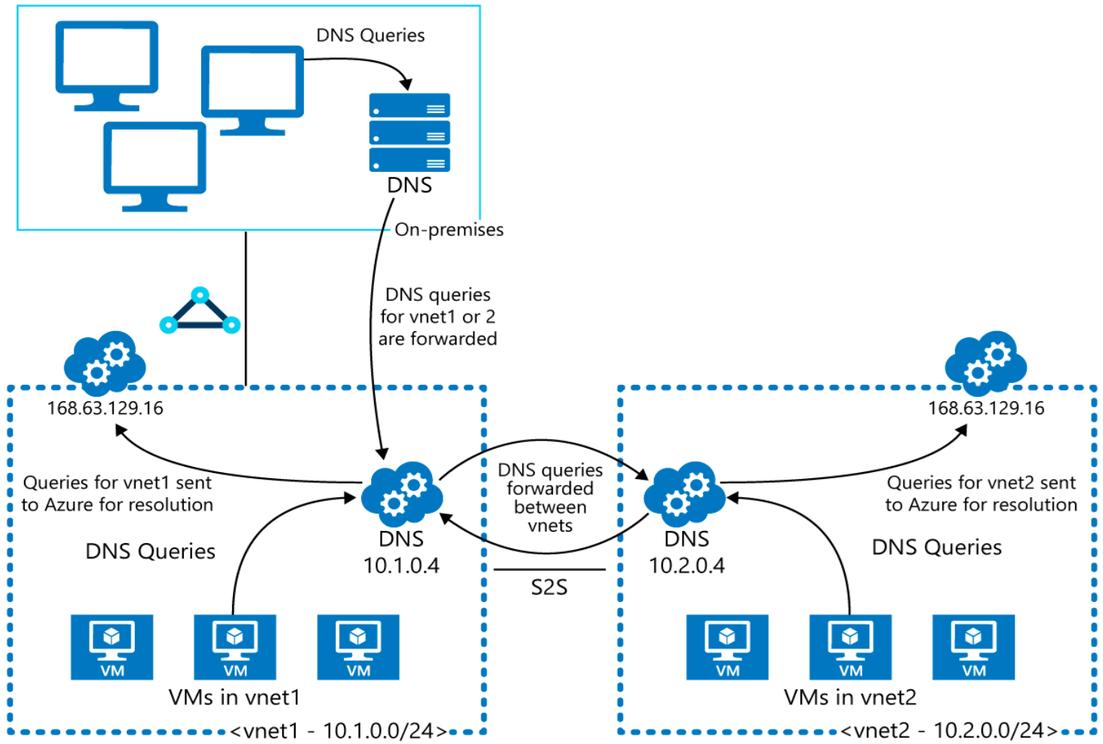
Name Resolution Using Customer-Provided DNS Server

DNS forwarding enables DNS resolution between virtual networks, allowing on-premises machines to resolve Azure-provided hostnames.



Name Resolution Using Customer-Provided DNS Server

To resolve a VM's hostname, the DNS server VM must reside within the same virtual network and be configured to forward hostname queries to Azure.

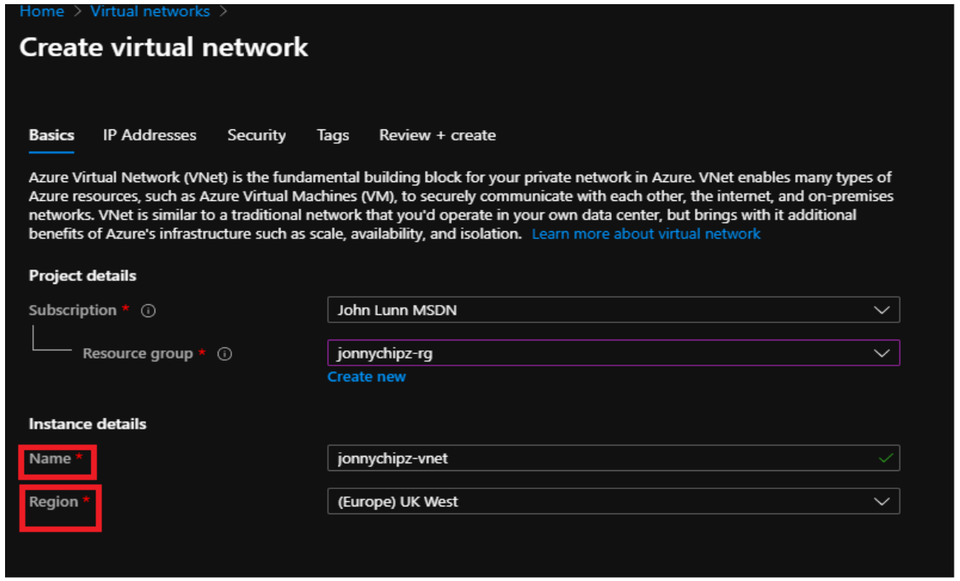


Use conditional forwarding rules to send DNS queries to the correct virtual network for resolution as each virtual network's DNS suffix is different.

Recommend a Solution for Network Provisioning

Naming and Regions

Each Azure resource has a unique name. Within a scope, the name must be unique, which varies depending on the resource type.



An Azure region produces all Azure resources. Only a virtual network in the same region can create a resource.

Segmentation

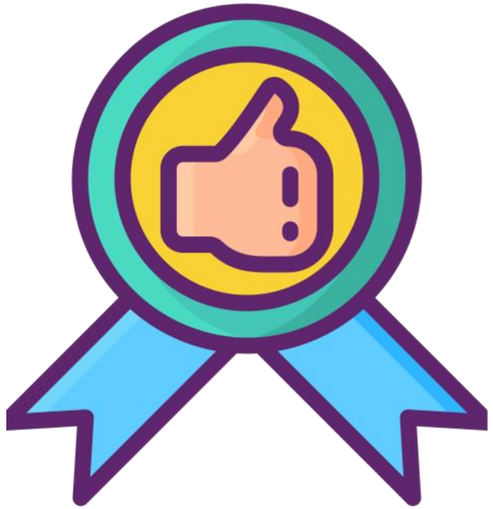
These are the segmentation considerations:

- The user can construct many virtual networks per subscription and location.
- Within each virtual network, the user can construct several subnets.
- Azure routes network traffic between all subnets in a virtual network.
- A virtual network can be split into two or more subnets up to the constraints.

Permissions and Policy

- Permissions are allowed for the management group, subscription, resource group, and individual resources.
- The user can create, assign, and manage policy definitions using Azure Policy.
- Azure Policy evaluates the resources of the user that are not compliant with the policy definitions.

Virtual Network Best Practices



- Ensure nonoverlapping address space
- Ensure that the entire VNet address space is not covered
- Configure a few larger VNets rather than many small ones
- Secure VNets by assigning Network Security Groups to subnets

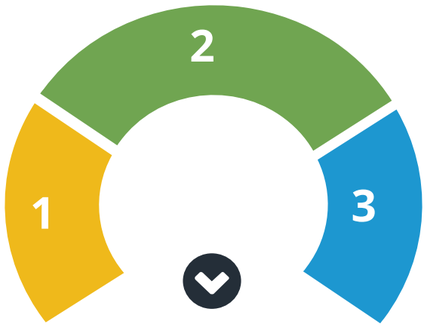
Recommend Solutions for Network Security

Network Security

Network security protects the communication of resources within and outside of a network.

Secures traffic flow between applications and the internet

Secures traffic flow amongst applications



Secures traffic flow between users and the applications

Focus Areas

Filter Network Traffic

Network Security Groups (NSG)

Network Virtual Appliances (NVA)

Network traffic filtration options

Route Network Traffic

By default, Azure routes traffic between subnets, connected virtual networks, on-premise networks, and the Internet.

To override the default rules, the following can be used:

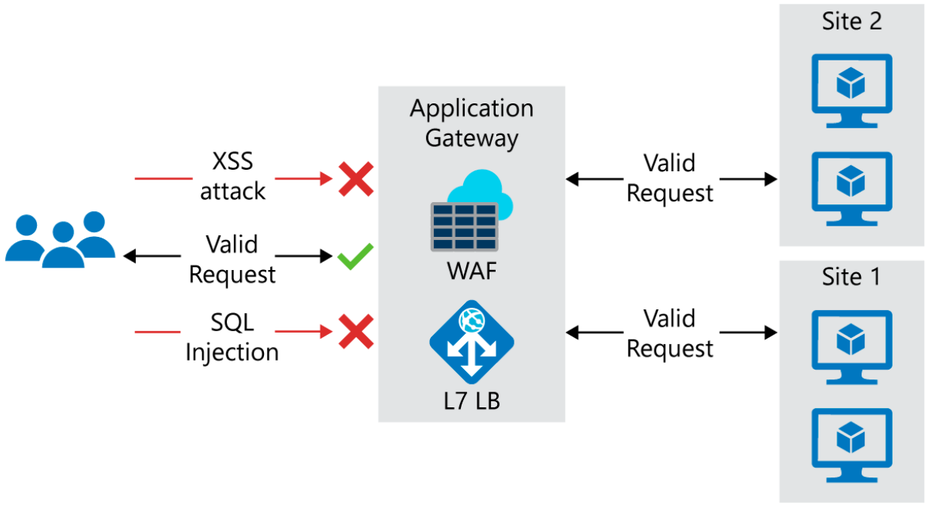
Route tables

A custom Route table with routes that control where traffic is routed can be created for each subnet.

Border Gateway Protocol (BGP) routes

An on-premise BGP route can be propagated to a VNet if a user links the VNet to an on-premise network. They can be linked through an Azure VPN Gateway or an ExpressRoute connection.

Internet Protection

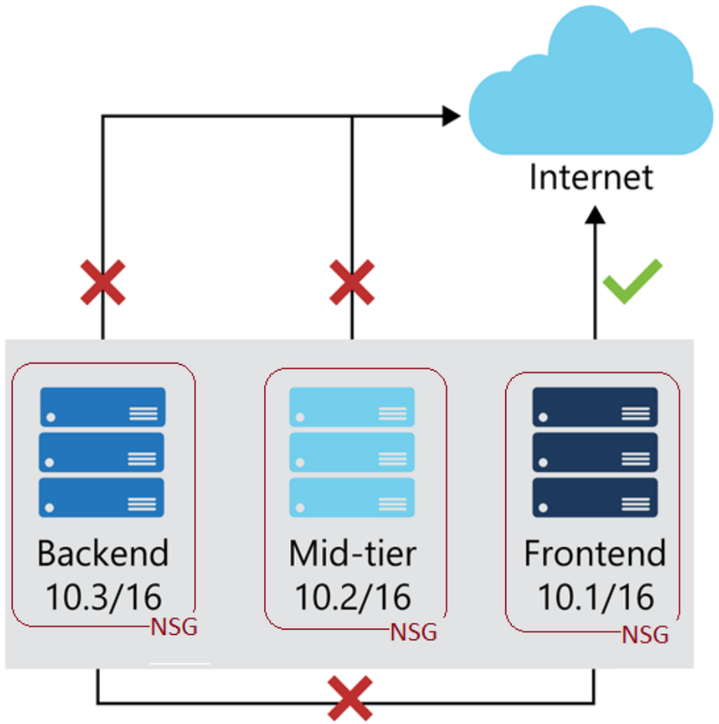


Different ways of restricting traffic from the internet:

- Identify resources that are allowing inbound network
- Use Azure Security Center
- Use an Application Gateway

Virtual Network Security

In an Azure virtual network, a user can use an Azure Network Security Group (NSG) to filter network traffic to and from Azure resources.



A user can use virtual network service endpoints to isolate services, enabling communication between virtual networks.

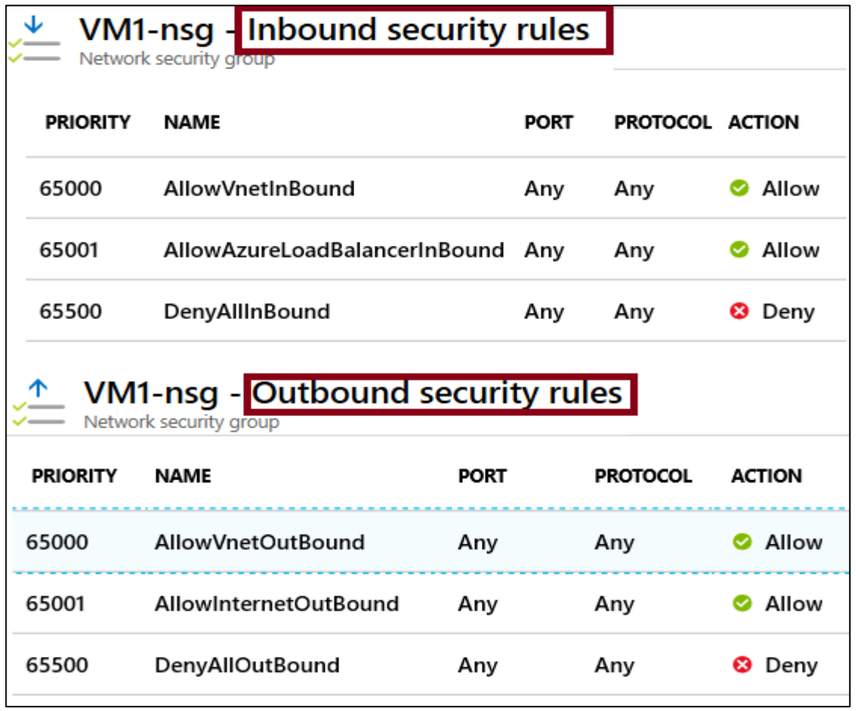
Network Security Group (NSG)

Features

- NSGs enable a user to limit network traffic to resources in a virtual network.
- NSG contains a list of security rules that allow or deny inbound or outbound network traffic.
- NSGs can be associated with a subnet or a network interface.
- NSGs operate in layers 3 and 4, allowing communication between network interfaces.
- NSGs are used to isolate applications between environments, tiers, and services.
- NSGs lock down network communication between virtual machines.

Network Security Groups' Rules

Security rules in NSGs enable a user to filter network traffic that can flow in and out of virtual network subnets and network interfaces.



VM1-nsg - Inbound security rules

Network security group

PRIORITY	NAME	PORT	PROTOCOL	ACTION
65000	AllowVnetInBound	Any	Any	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	Allow
65500	DenyAllInBound	Any	Any	Deny

VM1-nsg - Outbound security rules

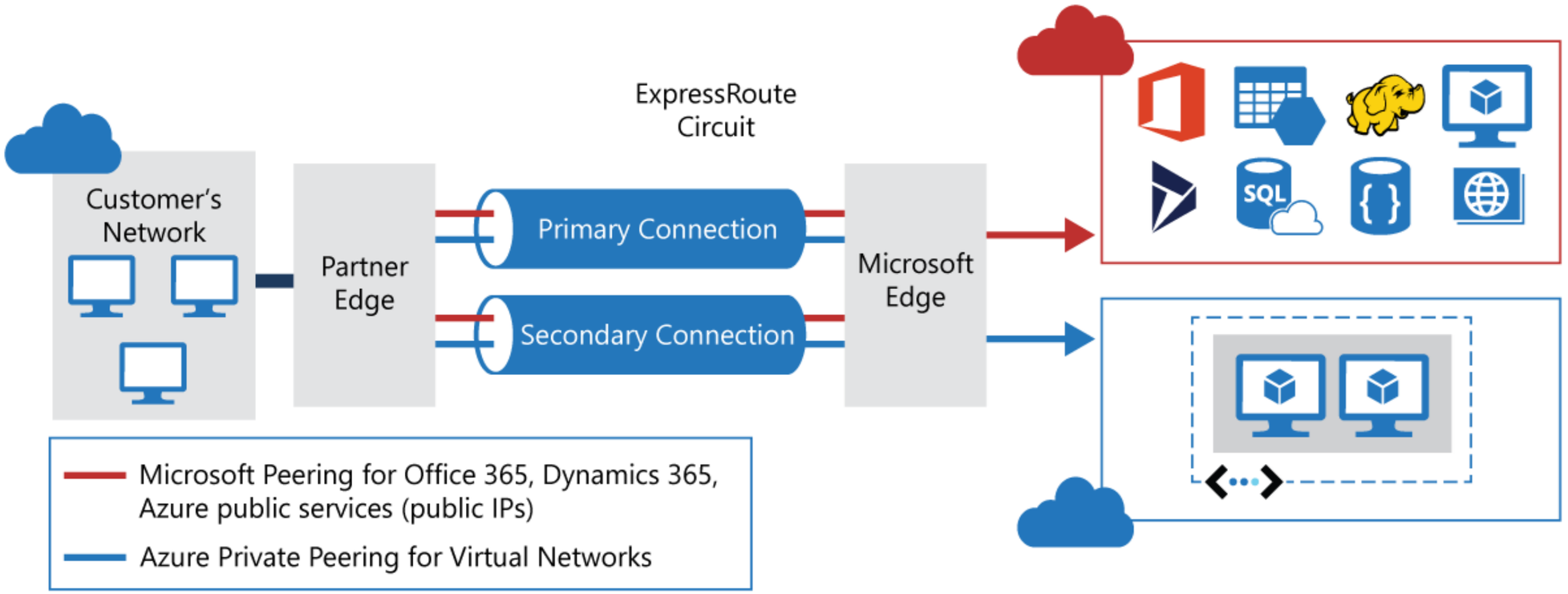
Network security group

PRIORITY	NAME	PORT	PROTOCOL	ACTION
65000	AllowVnetOutBound	Any	Any	Allow
65001	AllowInternetOutBound	Any	Any	Allow
65500	DenyAllOutBound	Any	Any	Deny

There are default security rules. A user cannot delete the default rules but can add other rules with higher priority.

Network Integration

VPN Connection, Express Route, and VNet Peering are generally used for providing integration between virtual networks.



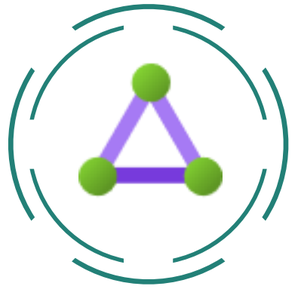
Recommend Solutions for Network Connectivity

Virtual Network Connectivity

There are different ways to allow network connectivity between virtual networks:

Vnet Peering

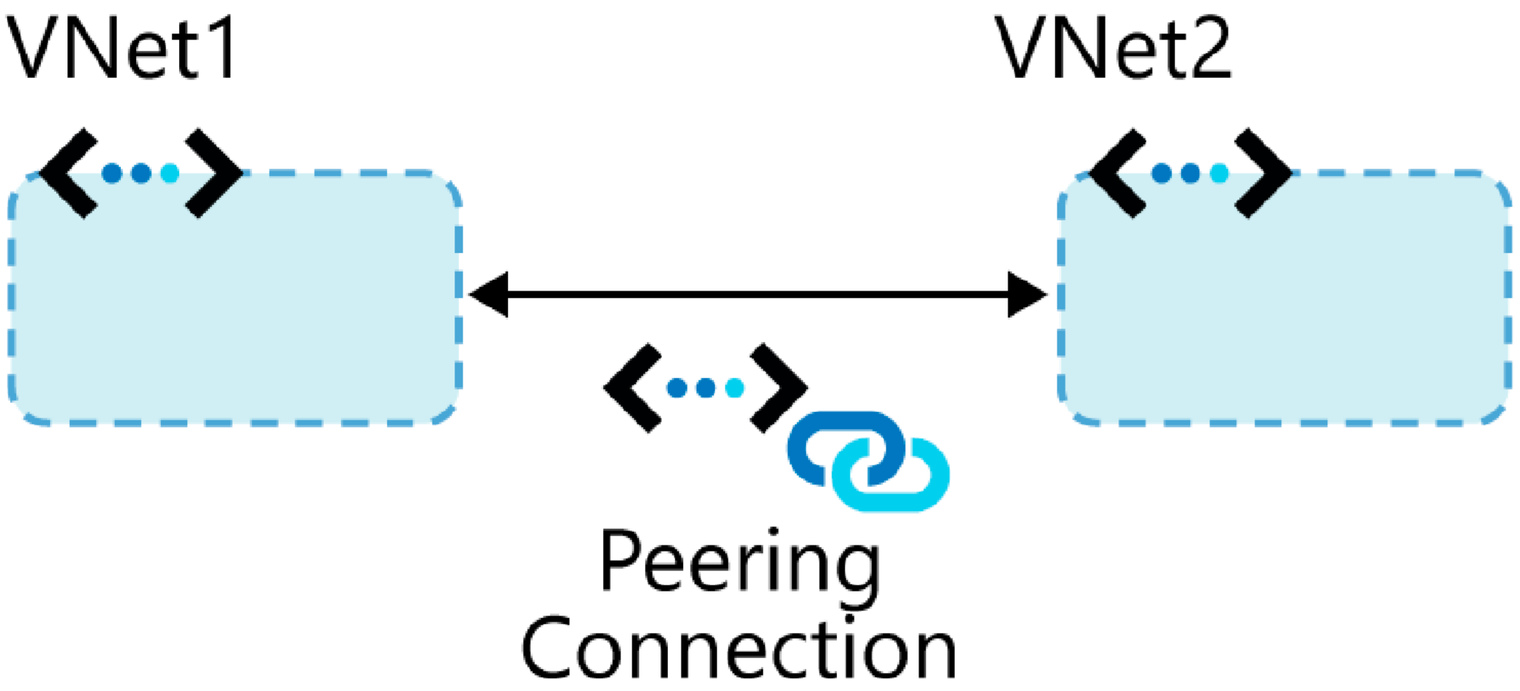
VPN Gateway Connections



ExpressRoute

Virtual Network Peering

Virtual network (VNet) peering connects two Azure virtual networks.



Virtual Network Peering Types

There are two types of peering connection:

Virtual network peering

Connects virtual networks in the same Azure region
Example: Connecting two virtual networks in North Europe

Global virtual network peering

Connects virtual networks present in different Azure regions
Example: Connecting a virtual network in North Europe and a virtual network in West Europe

Peering Considerations

Keep the following in mind for VNet peering:

Reciprocal connections:

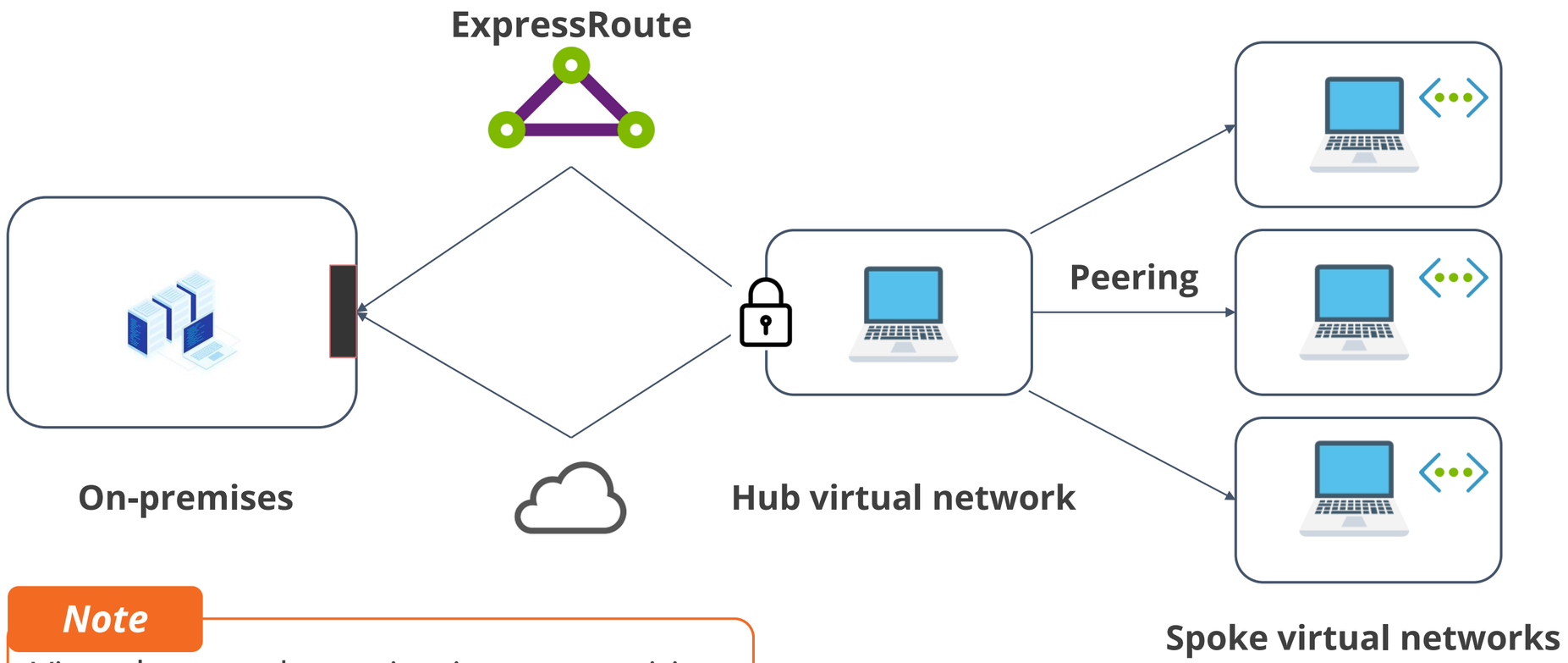
A user must establish a connection on each virtual network to link the networks while using virtual network peering.

Cross-subscription connections:

Virtual network peering can be done even when both virtual networks are in different subscriptions.

Transitivity

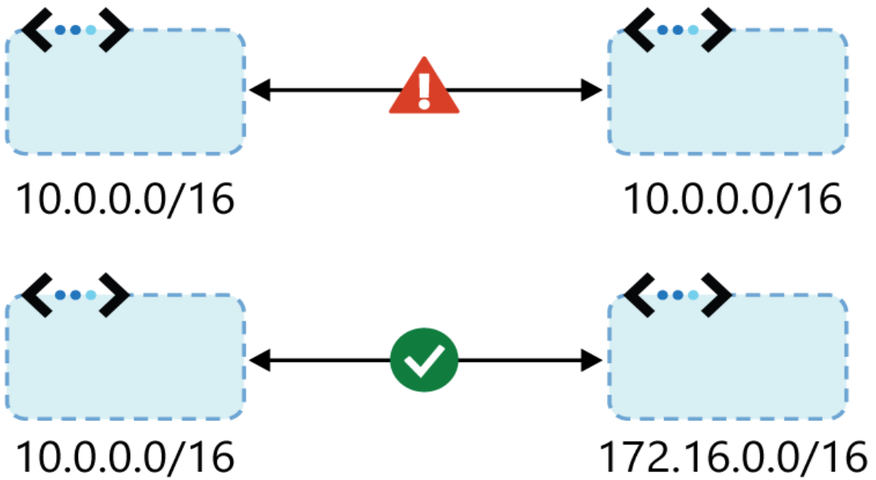
Peer-to-peer transitive routing is a concept used in Azure to describe network traffic that is routed via an intermediary virtual network between two virtual networks.



Note

Virtual network peering is nontransitive.

Gateway Transit



Benefits

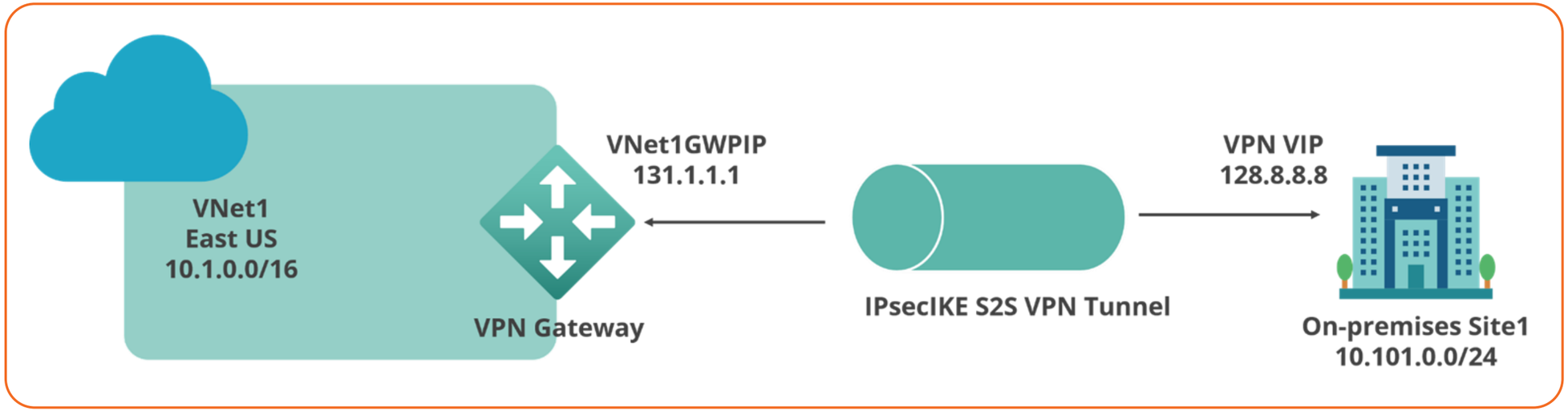
- Facilitate cross-premise connectivity
- Enable the allow gateway transit option in the hub
- Enable the use remote gateway option on the spoke

Peering considerations

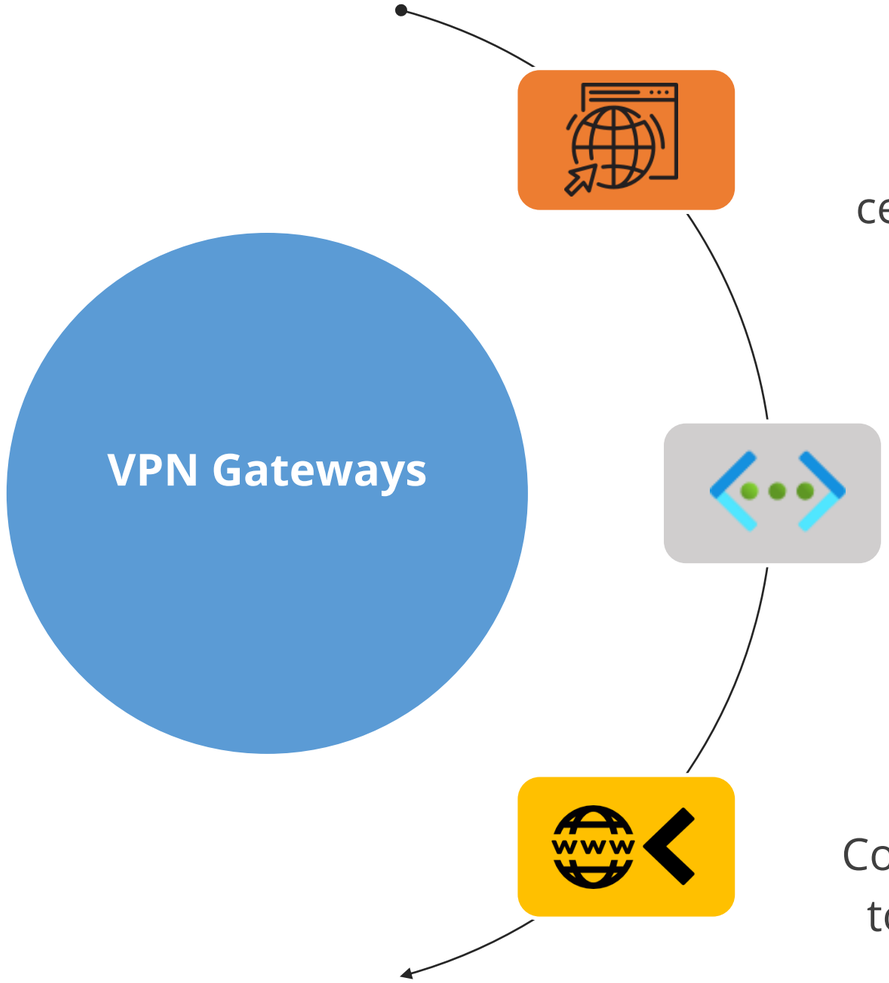
- IP address spaces should not overlap
- Peering is the recommended option

VPN Gateways

VPN gateways provide cross-premises connectivity between customer premises and Azure.



VPN Gateways Types



Site-to-Site
Connects on-premises data centers to Azure virtual networks

Vnet-to-Vnet
Connects Azure virtual networks (custom)

Point-to-Site
Connects individual devices to Azure virtual networks

VNet Peering and VPN Gateways

VNet peering

- Is direct (no interconnecting device)
- Has low latency and high bandwidth
- Is regional or global

VPN gateway

- Serves as an interconnecting devices
- Introduces extra latency and limits bandwidth

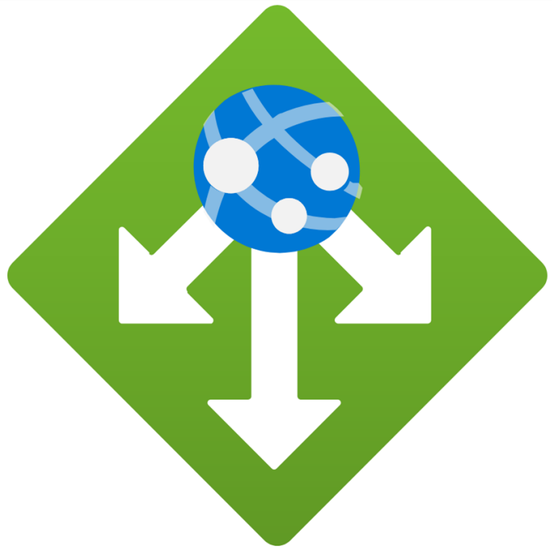
Gateway transit

- Allows sharing a VPN or ExpressRoute gateway across a peering
- Minimizes complexity and centralizes management

VNet Peering Versus VPN Gateways

Item	Virtual network peering	VPN gateway
Limits	Up to 500 per VNet	One per VNet (per gateway limits are SKU dependent)
Pricing model	Ingress/Egress	Hourly + Egress
Encryption	Not included	IPsec/IKE
Bandwidth	No limits	SKU-dependent
Public endpoints	No	Yes
Transitivity	No	Yes (routing dependent)
Initial setup time	Fast	30 minutes
Typical scenarios	Data replication, database failover, and other scenarios needing frequent backups of large data	Encryption-specific scenarios are not latency sensitive and do not need high power

VNet Peering Versus VPN Gateways

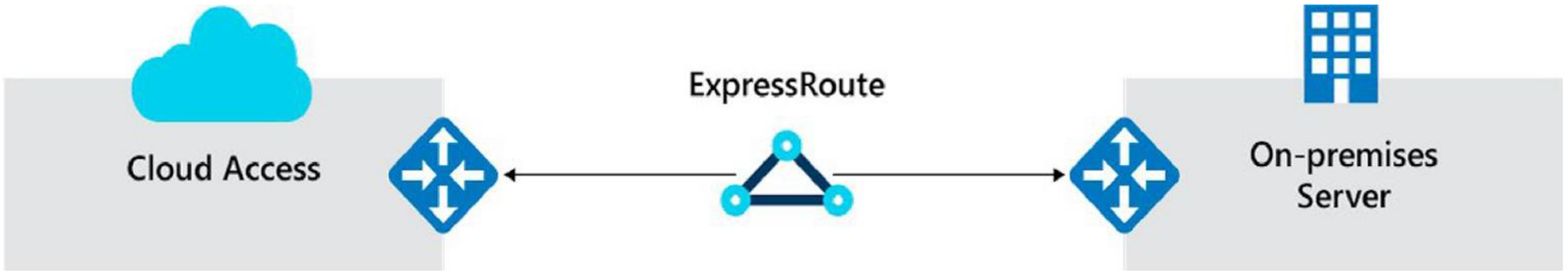


Virtual Network peering and VPN gateways support connecting:

- Virtual networks in different regions
- Virtual networks in different Azure Active Directory tenants
- Virtual networks in different Azure subscriptions
- Virtual networks that use a mix of Azure deployment models

Azure ExpressRoute for Hybrid Networks

Azure ExpressRoute is an Azure service that allows the user to extend on-premises networks over a private connection with the help of a network.



ExpressRoute Circuits

A Circuit is an ExpressRoute logical connection between an on-premises network and an Azure network.

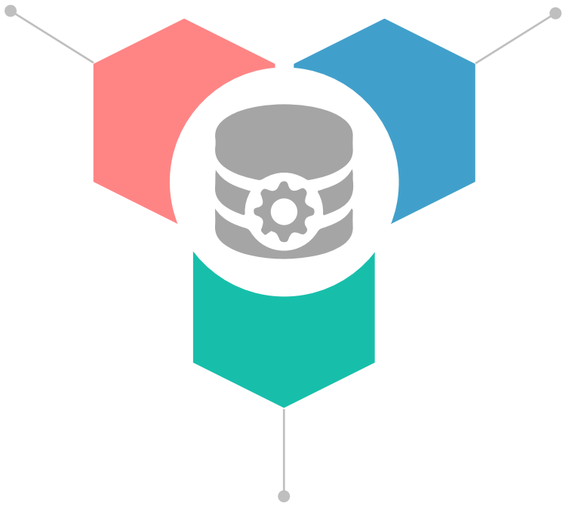
Benefits

- It configures traffic management and routing in ExpressRoute using circuits.
- It supports multiple circuits across various regions.
- It supports connections using various connectivity providers.
- It supports multiple routing domains and peering.
- It does not need physical mapping.

ExpressRoute Circuits

Azure private peering

- Trusted extension of the core network in Azure with bidirectional connectivity



Circuit bandwidth

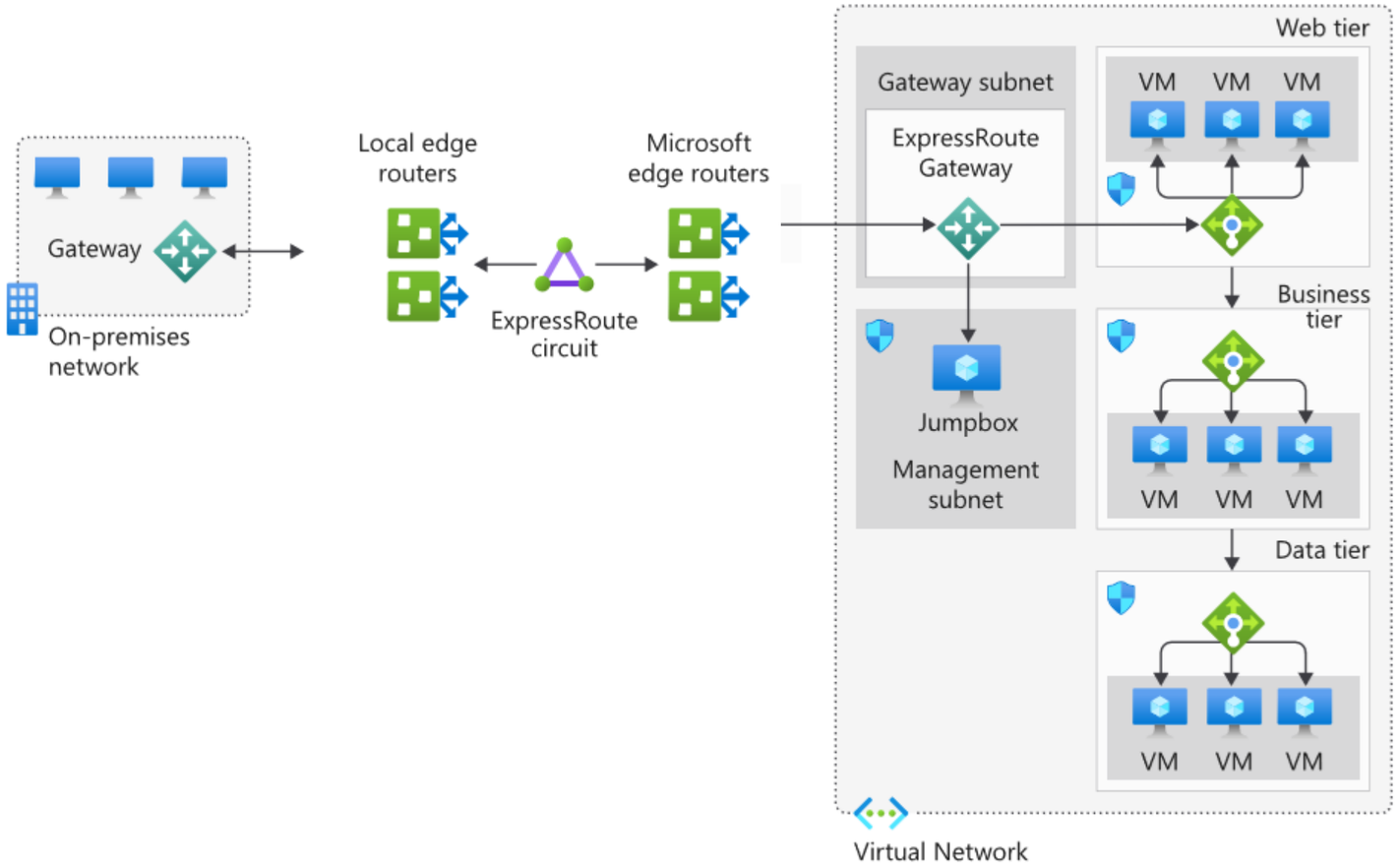
- Have as many circuits as the user needs to match bandwidth requirements

Microsoft peering

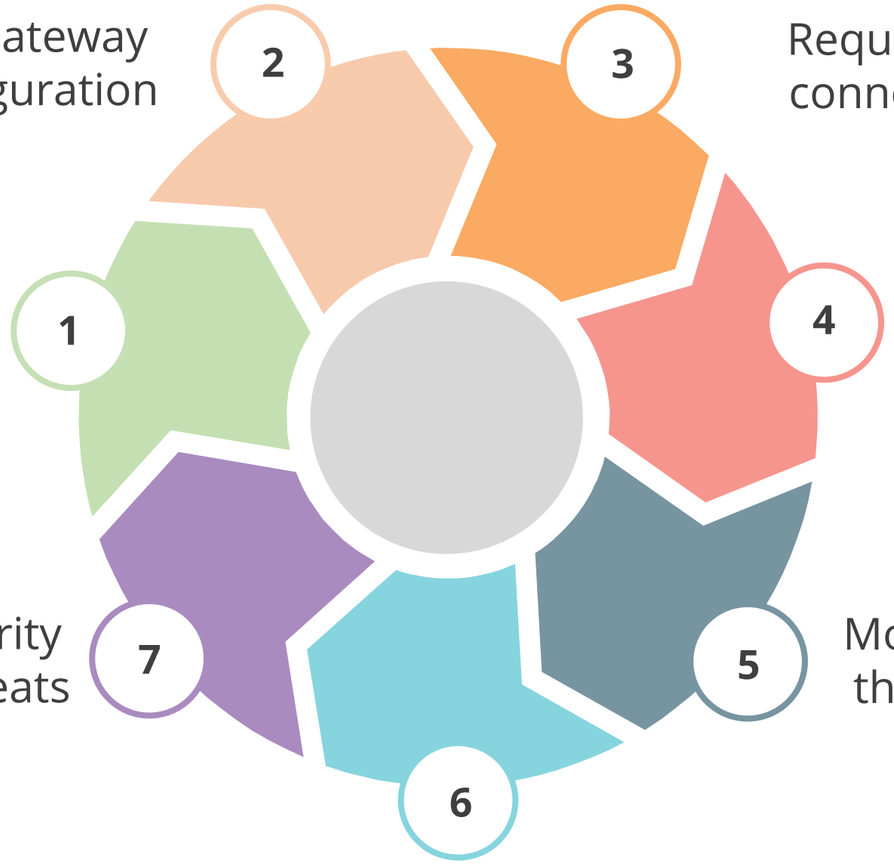
- Provides connectivity to all Microsoft online services
- Requires a public IP address

ExpressRoute Reference Architecture

The following figure shows the architecture of how ExpressRoute works:



ExpressRoute Considerations



1. Supports circuit management by the connectivity provider
2. Requires a Border Gateway Protocol (BGP) configuration
3. Requires working with connectivity providers
4. Requires on-premises high-bandwidth routers
5. Monitors the connectivity using the Azure Connectivity Toolkit
6. Requires network security appliances between the routers and networks
7. Requires a network security appliance to manage threats

Service Endpoint

The VNet service endpoint allows secure and direct access to Azure services via an efficient path across the Azure backbone network.

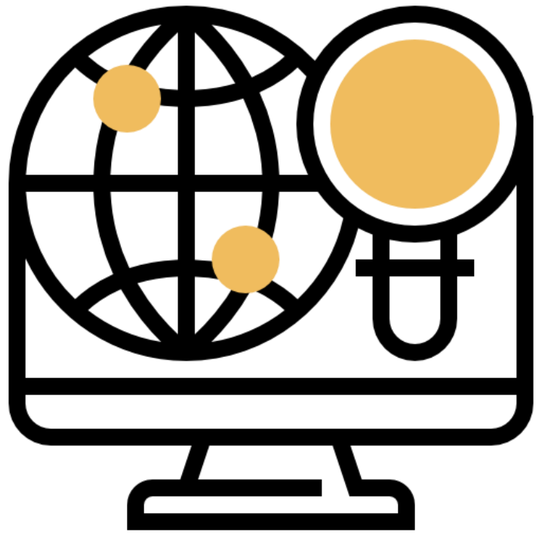
Endpoints allow the user to limit access of Azure service resources to their virtual network exclusively.

Service Endpoint Benefits

Benefits	Explanation
Improved security for Azure service resources	By extending the VNet identity to Azure service endpoints, users may secure Azure service resources to user's virtual network.
Optimal routing for Azure service traffic from the virtual network	Service traffic is always routed directly from the user's virtual network to the service on the Microsoft Azure backbone network by endpoints.
Simple to setup with less management overhead	Service endpoints do not require any Network Address Translation (NAT) or gateway devices to be set up.

Private Link

Azure Private Link allows a user to use a private endpoint in user virtual network to access Azure PaaS Services as well as Azure hosted customers-owned or partner services.



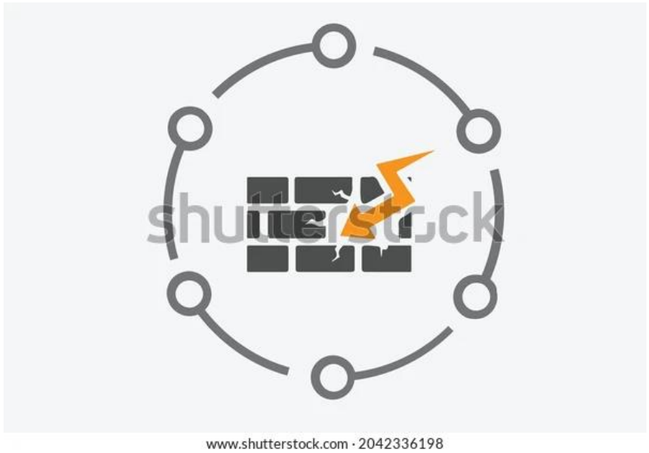
Azure Private Link’s setup and consumption are consistent across Azure PaaS, customer-owned and shared partner services.

Private Link Benefits

Benefits	Explanation
Privately access services on Azure platform	Azure backbone network is used to link the customer to the services, which will be handled by the Private Link Platform
On-premises and peered networks	Users must access Azure services from on-premises utilizing private endpoints, ExpressRoute private peering, VPN tunnels, and peered virtual networks.
Protection against data leakage	Private endpoint is associated with a PaaS resource instance rather than the entire service.
Global Reach	It helps to connect to services securely in other parts of the world.

Private Endpoint

A private endpoint is a network interface that connects to a user virtual network using a private IP Address.



This network interface connects users to a service powered by Azure Private Link in a private and secured manner.

Network Security of Private Endpoints

- Traffic is secured to a private link resource when private endpoints are used.
- The platform performs access control to ensure that network connections only go to the private link resource defined.

- It prevents workloads from connecting to a supported Azure service via public endpoints.
- It prohibits access to other Azure resources that are hosted on the same Azure service.

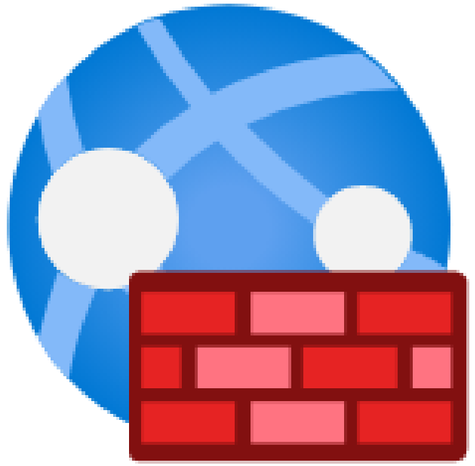
Web Application Firewalls (WAFs)

WAFs provide online applications with a basic level of protection. It provides additional defense-in-depth mitigation.

WAFs help to reduce the chances of an attacker exploiting common application security flaws.

Web Application Firewalls (WAFs)

This mechanism is an important mitigation because attackers target web applications as an entry point into an organization.



- WAF capabilities in Azure Application Gateway inspect web traffic and threats in the HTTP layer.
- It is a load balancer and HTTP(S) complete reverse proxy that can encrypt and decrypt secure socket layer (SSL) traffic.

Azure Firewall

Azure Firewall is a cloud-native, intelligent network firewall security service that offers best threat prevention for user Azure workloads.

- It protects the virtual network against potentially harmful traffic from the internet and other sources.
- It inspects incoming traffic and allows only those requests to proceed.

DDoS Attacks

In a Distributed Denial-of-Service (DDoS) attack, the server is overloaded with bogus traffic.

This attack can completely shut down or block access to services.

Implementation of DDOS Protection

Let's see some considerations :

- DDOS assaults are already protected by Azure Infrastructure.
- For services provisioned via virtual network, Azure provides additional security in the network.

- Features such as machine learning-based monitoring approaches must be considered for detecting unusual traffic.
- User application must be protected before it suffers a service degradation.

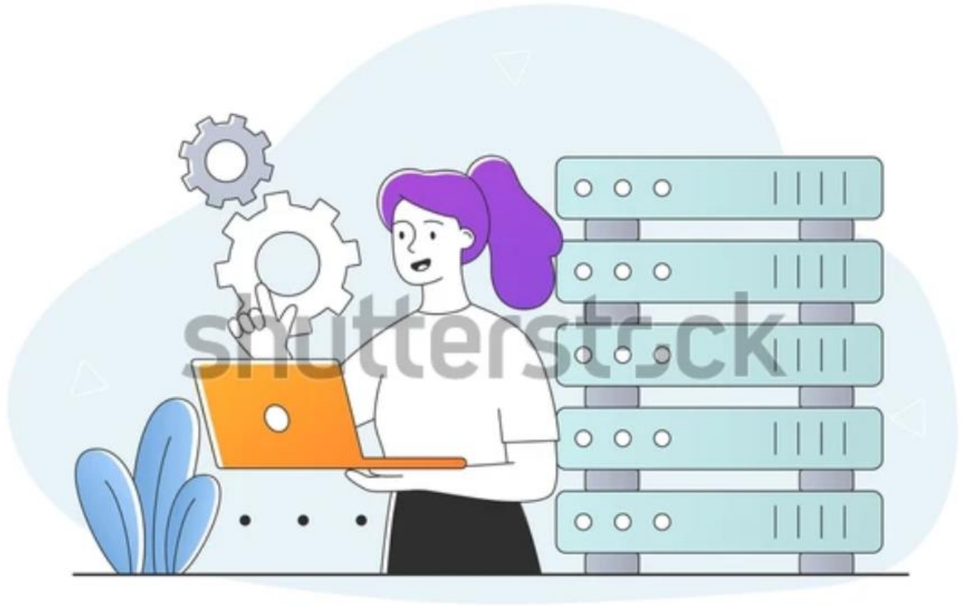
Azure Bastion

Bastion is a fully managed platform as a service (PaaS) that users install in a virtual network.

It allows secure and smooth RDP and SSH communication to the user's virtual network’s VMs through TLS, directly from the Azure portal.

Just-In-Time Access

JIT VM access is a Defender for Cloud feature that gives network-based access to VMs on time.



This feature secures the VM network interface or the subnet that contains the VM network interface by adding a deny rule to the Azure network security group.

Assisted Practice

Creating Virtual Networking and Resolving Domain Names

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been asked to create a virtual network in Azure that will host virtual machines. Also, you need to deploy them into different subnets of the virtual network and you need to implement DNS name resolution for Azure virtual machines within the virtual network.

Assisted Practice: Guidelines

Steps to resolve domain names are:

1. Login to your Azure portal
2. Create a virtual network
3. Create a subnet
4. Create a public IP address and the network interface
5. Create the network security group

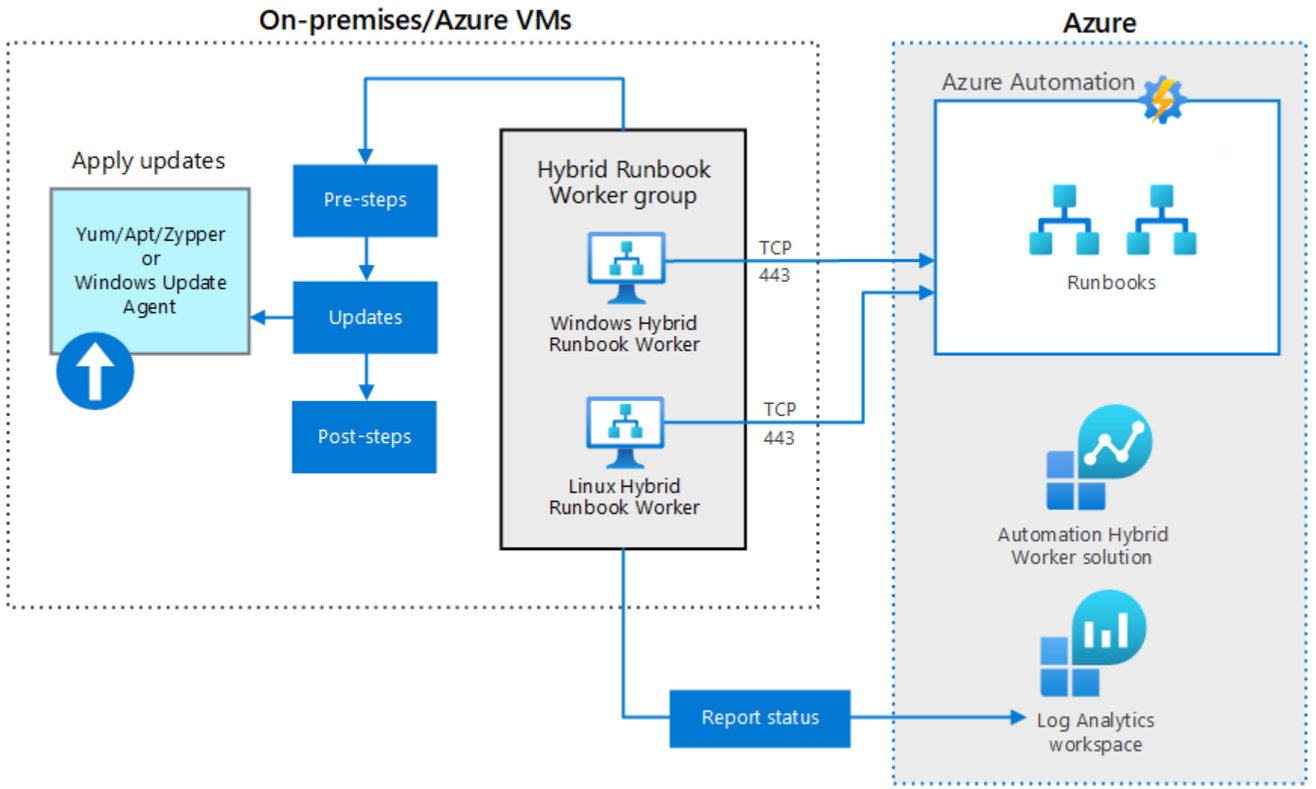
Recommend Solutions for Automating Network Management

Azure Automation Update Management

Update Management is a feature of Azure automation that allows the user to handle operating system upgrades for virtual machines in Azure, on-premises, and other cloud environments.

Hybrid Update Management Architecture

The following diagram shows the architecture of hybrid update management:



Use Cases of Architecture

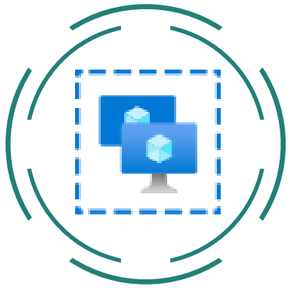
The hybrid update management architecture is used for:

- Managing updates across on-premises and in Azure using the Update Management component of Automation Account
- Using scheduled deployments to orchestrate the installation of updates within a defined maintenance window

Update Management Considerations

These are the considerations for Update Management:

Scalability considerations



Availability considerations

Recommend Solutions for Load Balancing and Traffic Routing

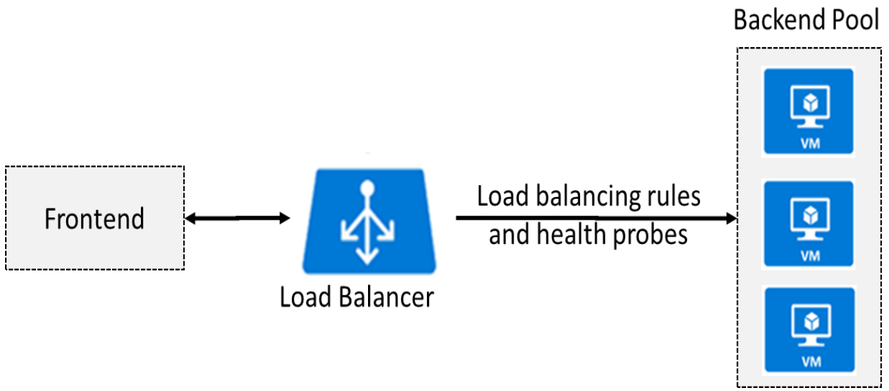
Load Balancing and Traffic Routing

Azure offers these services for managing network traffic distribution and load balancing:

Based on the user's demands, they can use these services individually or in combination to create the best solution.

Azure Load Balancer

Load Balancer distributes inbound traffic to backend resources.



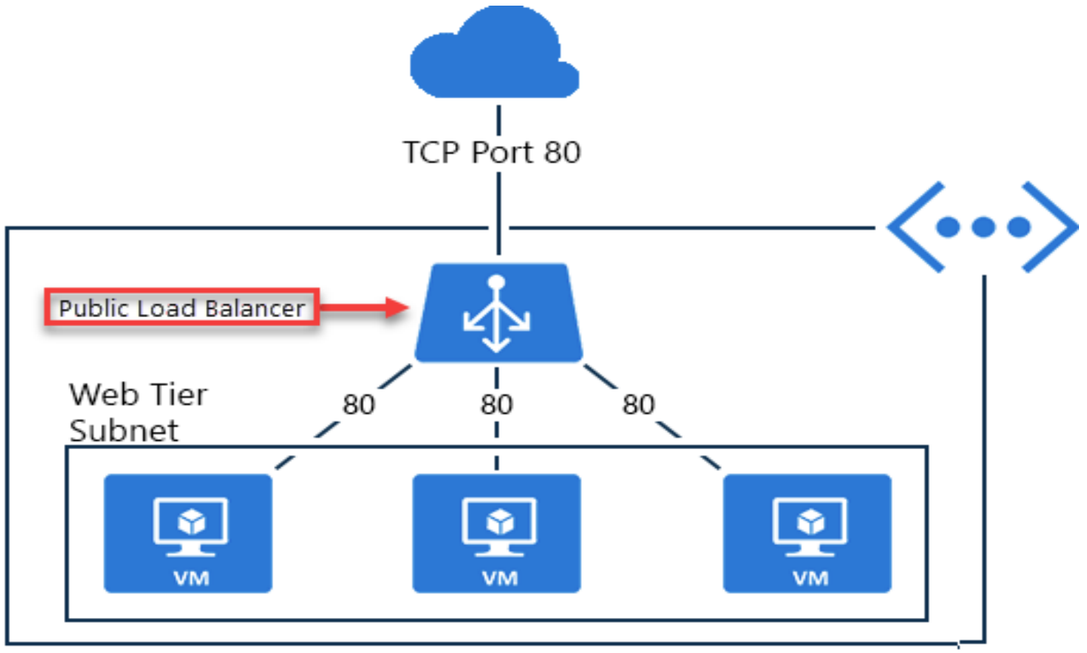
The on-premises web applications are protected with secure remote access.

Azure Load Balancer

Azure Load Balancer is of two types:

Public Load Balancer

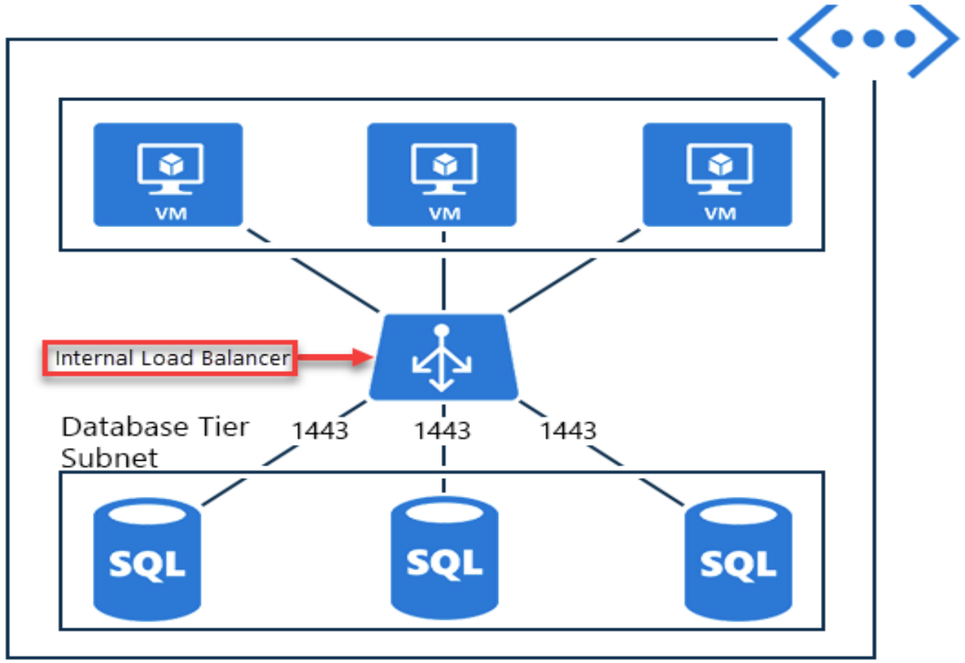
Public load balancer maps public IP addresses and port numbers of incoming traffic to the VM's private IP address and port number and vice versa.



It applies load balancing rules to distribute traffic across VMs or services.

Internal Load Balancer

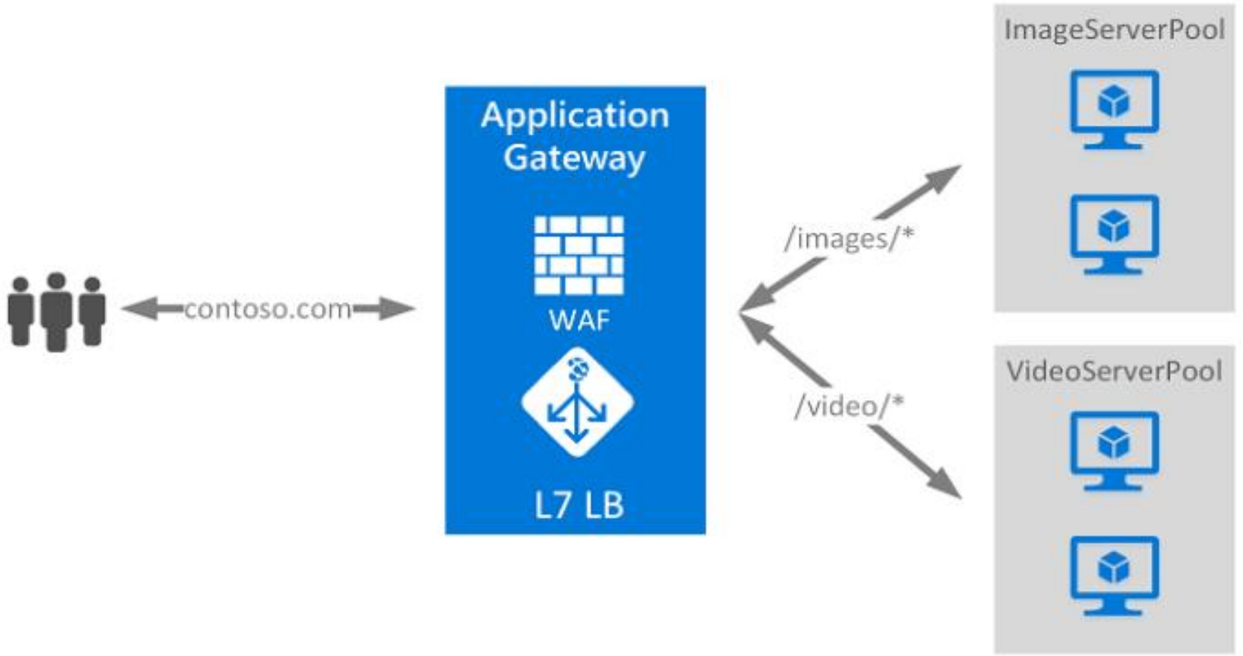
Internal load balancer directs traffic only to resources inside a virtual network or those that use a VPN to access Azure infrastructure.



It enables load balancing within a virtual network for cross-premises virtual networks, multi-tier applications, and line-of-business applications.

Application Gateway

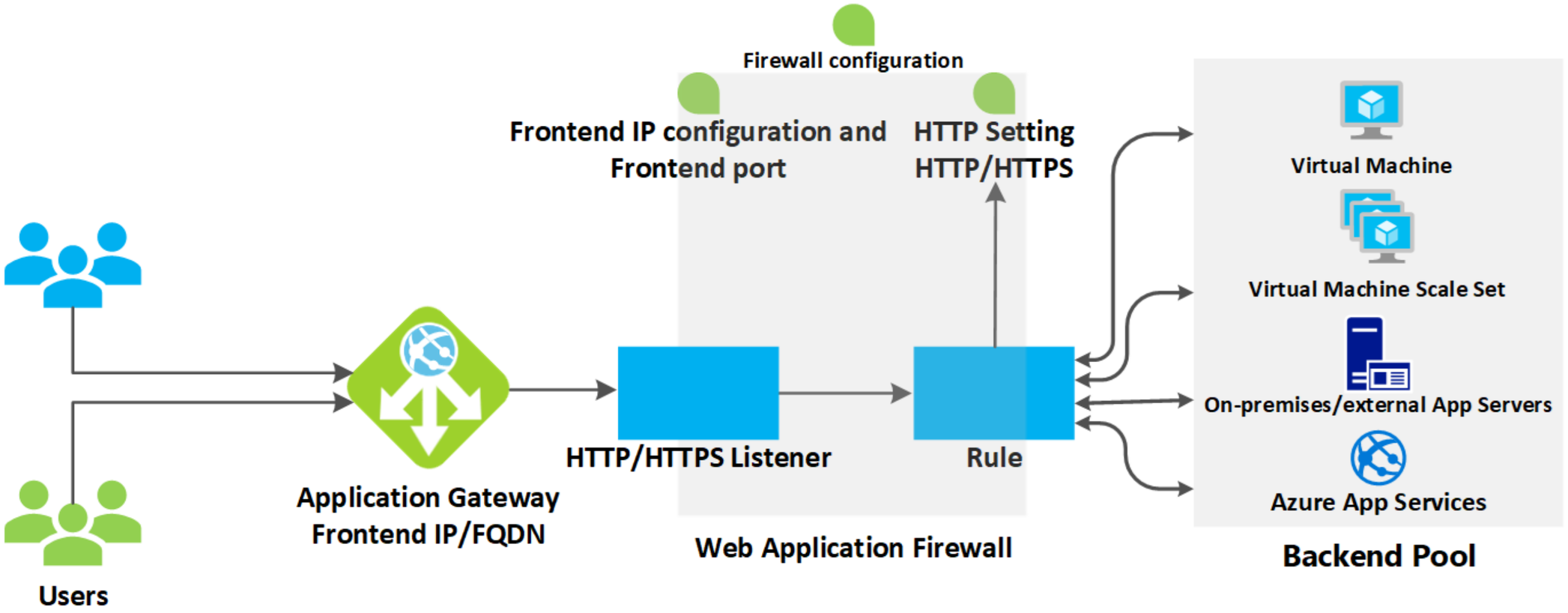
Application gateway controls the queries that clients can make to a web application.



It sends traffic to a group of web servers based on the request's URL.

Application Gateway

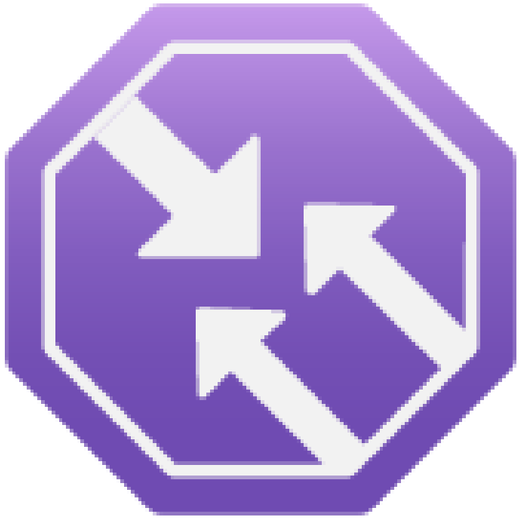
The workflow of Application Gateway is shown below:



Source: https://docs.microsoft.com/en-us/azure/application-gateway/how-application-gateway-works

Traffic Manager

Users are routed to web app endpoints (deployments) in potentially multiple data centers across the world using Traffic Manager, a network service.



Benefits

It ensures the apps are highly available and highly scalable.

Traffic Manager

These are the features of a traffic manager:

- Increases application availability
- Improves application performance
- Distributes traffic for complex deployments
- Maintains service without downtime
- Combines hybrid applications

Distributing Network Traffic

The network traffic table is explained below:

Service	Azure Load Balancer	Application Gateway	Traffic Manager	Azure Front Door
Technology	Transport layer (Level 4)	Transport layer (Layer 7)	DNS resolver	Layer 7 or HTTP/HTTPS
Protocols	Any TCP or UDP protocol	HTTP, HTTPS, HTTP/2, and web sockets	DNS resolution	Split TCP-based anycast protocol
Backends and endpoints	Azure VMs and Azure VM scale sets	Azure VMs, Azure VM scale sets, Azure app services, IP addresses, and hostnames	Azure cloud services, Azure app services, Azure app services slots, and public IP addresses	Internet-facing services hosted inside or outside of Azure
Network connectivity	External and Internal	External and Internal	External	External and Internal

Assisted Practice

Load Balancer **Duration: 10 Min.**

Problem Statement:

You've been asked to assist your organization with an Azure network solution that can be utilized to evenly distribute the load (incoming network traffic) across a collection of backend resources or servers as an Azure Architect. Your applications should be scalable, and you should be able to construct highly available services.

Assisted Practice: Guidelines

Steps to create a Load Balancer are:

1. Login to your Azure portal
2. Create a resource
3. Select the option of networking and click on the load balancer
4. Create the load balancer

Assisted Practice

Application Gateway

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been asked to assist your organization with an Azure Network solution, which can be used to manage traffic to your web apps and may make routing decisions based on additional attributes of an HTTP request, such as URI path or host headers.

Assisted Practice: Guidelines

Steps to create an application gateway are:

1. Login to your Azure portal
2. Create a resource
3. Navigate to the Application Gateway
4. Create an application gateway

Assisted Practice

VNet-to-VNet connection using VPN gateway

Duration: 10 Min.

Problem Statement:

Sim-Edu is a global firm with its headquarters in the US and branch offices in multiple other locations in the UK, Asia Pacific, etc. As part of their initial setup, they decided to leverage the hybrid connectivity options that Azure provides. They decided to use VPN Gateway to test connections between two virtual networks.

Assisted Practice: Guidelines

Steps to create an application gateway are:

1. Create virtual networks, gateways, and connections using an ARM template
2. Deploy virtual machines using other ARM templates
3. Test the connections

Assisted Practice

Implement Intersite Connectivity

Duration: 30 Min.

Problem Statement:

As an Azure Architect, you need to implement a lab environment with different networks with full connectivity between them and verify its functionality.

Assisted Practice: Guidelines

Steps to implement Intersite connectivity are:

1. Login to your Azure portal
2. Configure the local and global virtual network peering
3. Test Intersite connectivity

Assisted Practice

Manage High Availability with Application Gateway

Duration: 30 Min.

Problem Statement:

As an Azure Architect, you've been asked to identify different options for using multi-site routing with single application gateway.

Assisted Practice: Guidelines

Steps to create and manage multi-site routing with single application gateway:

1. Login to your Azure portal
2. Create a Virtual Network
3. Purchase DNS Names
4. Install Webservers on VMs using run commands
5. Create DNS Zones in Azure
6. Set up DNS Delegation in Azure
7. Create an Application Gateway using Portal with multi-site routing
8. Update DNS Zones
9. Test Applications

Key Takeaways

- Application gateway manages requests and routes traffic to a pool of web servers.
- Traffic Manager routes users to web app endpoints in potentially different data centers located around the world.
- Network security protects the communication of resources within and outside of your network.
- Azure Network Security Group (NSG) can be used to filter network traffic to and from Azure resources.

Design a Network Solution

Duration: 25 min.

Project Agenda: To design a network solution for the below scenario

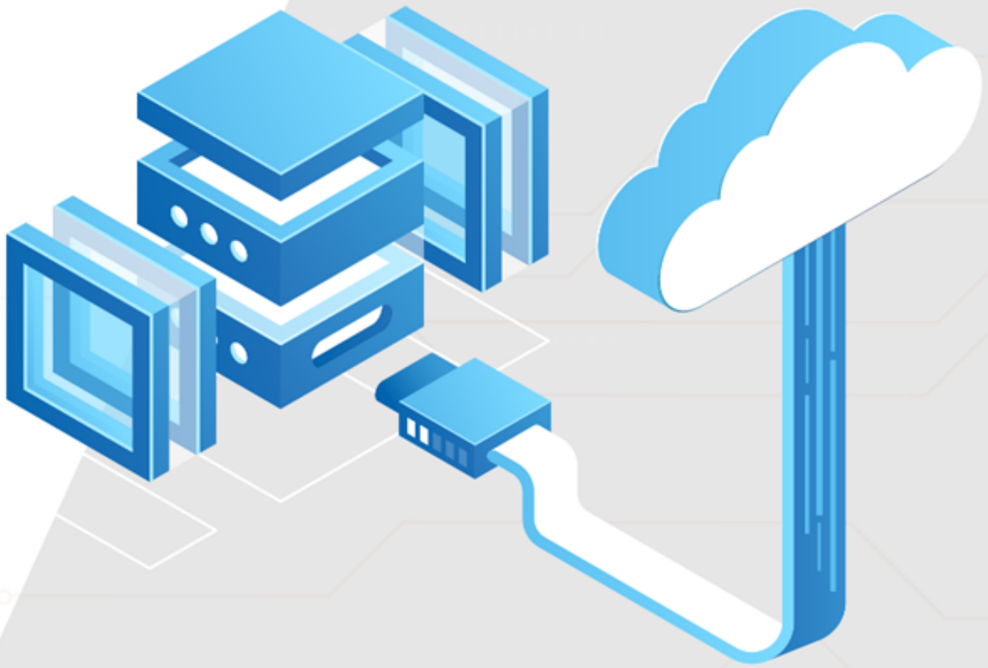
Objective: You are working as a principal engineer in an organization, and you have been asked to design a solution for an on-premise network to deploy a virtual appliance. The plan is to deploy multiple Azure VMs and connect the on-premises network to Azure using a site-to-site connection.

You also need to ensure that all the network traffic that will be directed from the Azure VMs to a specific subnet must flow through the virtual appliance. As part of compliance, the VMs should not access the internet as they store sensitive data. Recommend a design considering the above requirements.

Perform the following:

1. Logging in to the Azure portal
2. Creating a virtual network in the Azure portal
3. Deploying the virtual machine in the respective virtual network
4. Verifying the network security group of the virtual machine

LESSON-END PROJECT



Thank you