Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud Computing

Powered by simplilearn

Cloud Computing

Caltech | Center for Technology & Management Education

PG CC - Microsoft Azure Architect Design: AZ:304

Powerd 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 which is planning to migrate to the cloud and is looking for the below solutions:

- A solution that should enable the Azure resource’s 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.

A Day in the Life of an Azure Architect

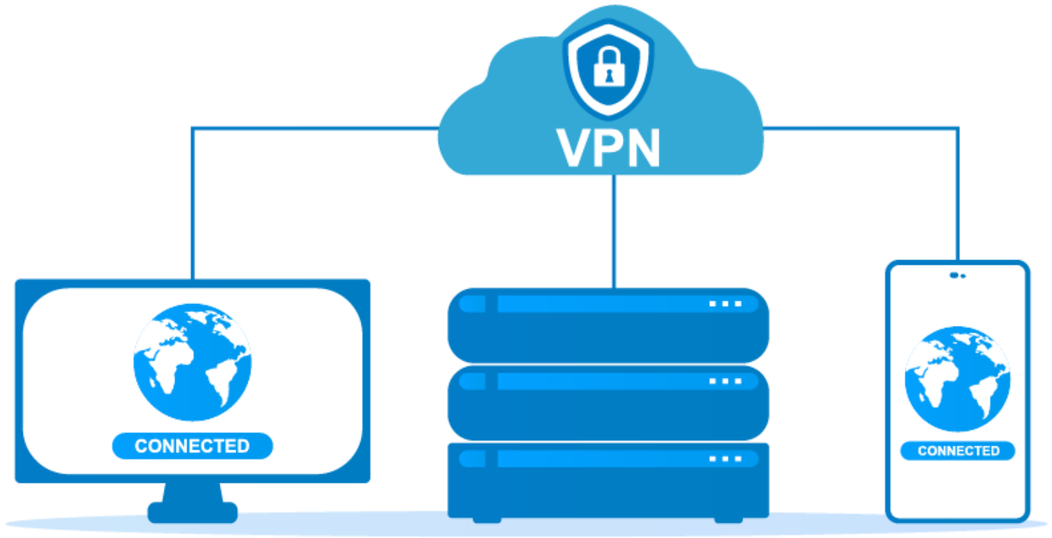
- Your applications should be scalable, and you should be able to construct highly available services.
- Your company is also looking for different types of networking solutions which can be used to manage traffic to your web apps and may make routing decisions based on various types of attributes such 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 your own network in the cloud.



VNets are used to 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.

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:

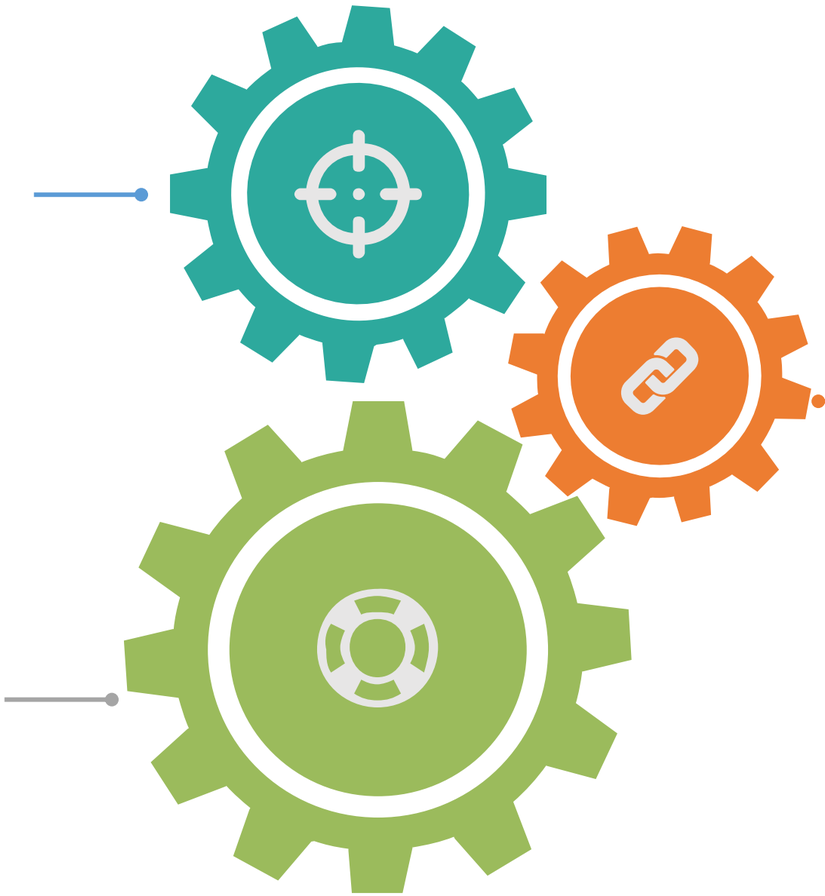
- Address space
- Subnet
- Region
- Subscription

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.



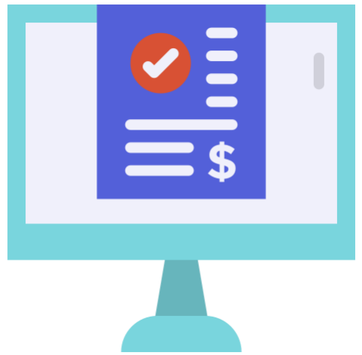
The hub can also be used as the connectivity point for your on-premises networks.

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

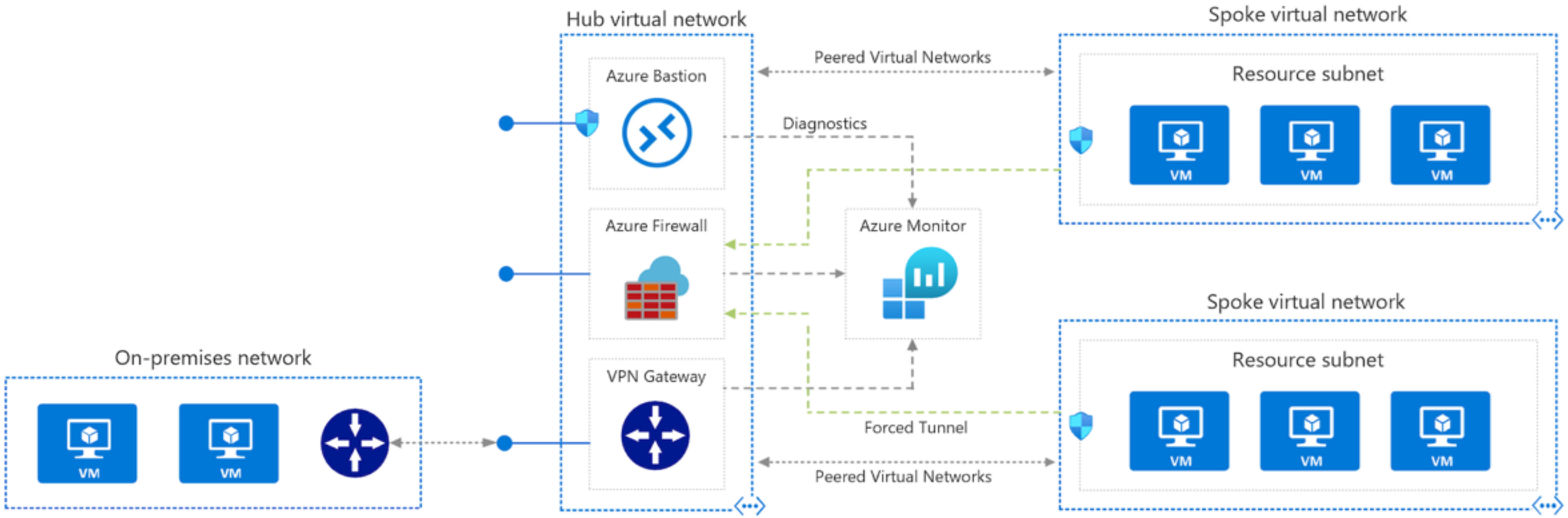


Overcoming subscription limit

Workload isolation

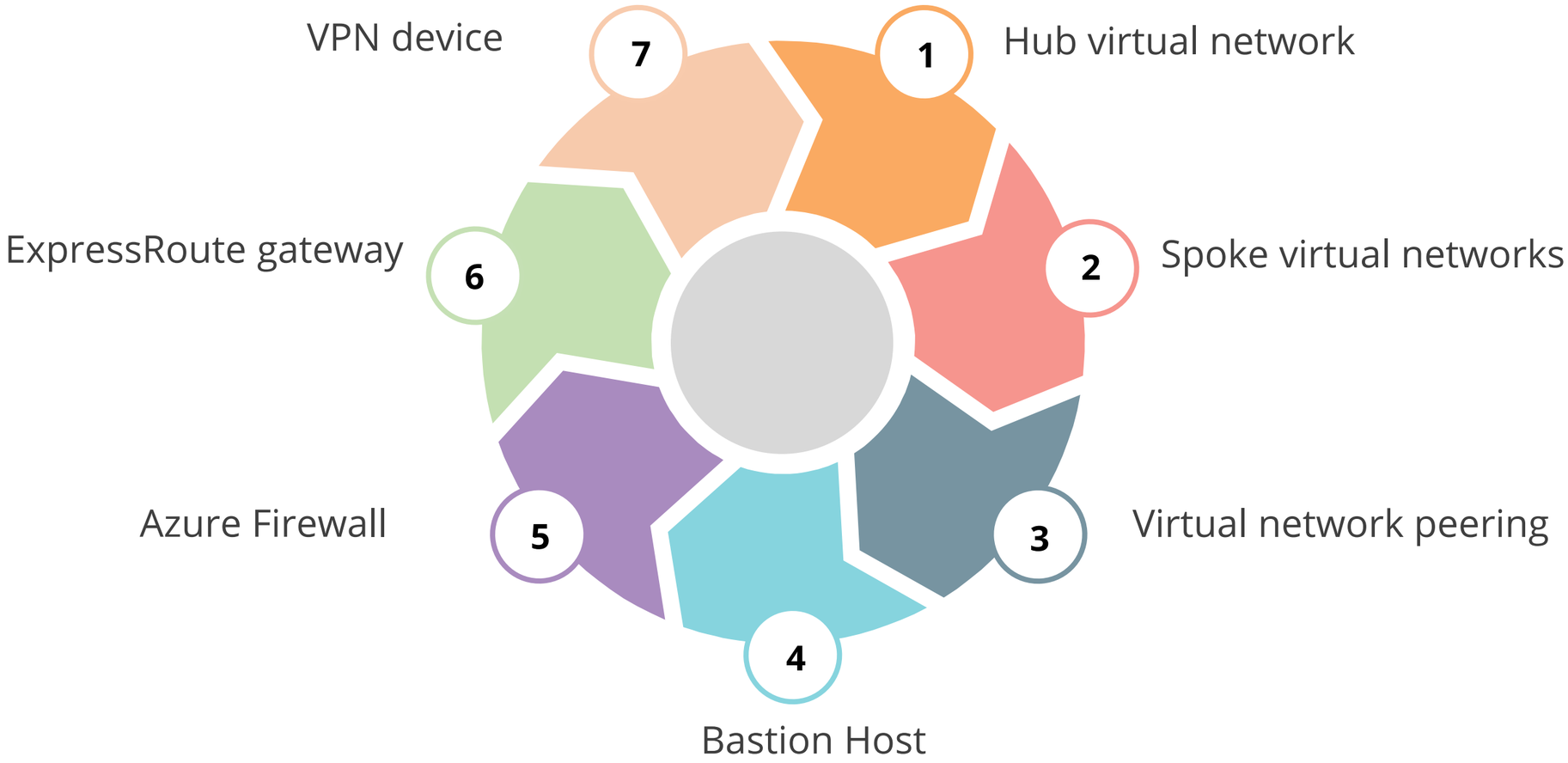
Hub and Spoke Architecture

Hub-spoke architecture is shown below:



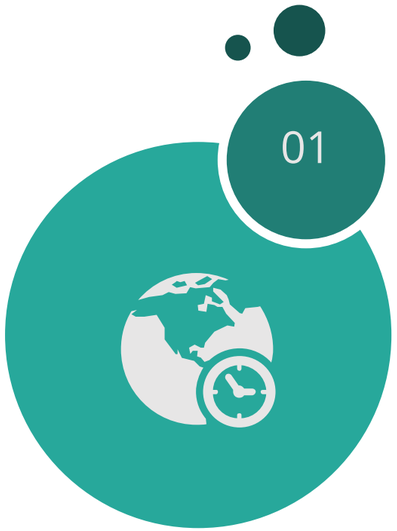
Components of Hub and Spoke Architecture

Hub-spoke architecture consists of the components below:



Use Cases of Hub and Spoke Architecture

Use cases of Hub-spoke architecture are given below:



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

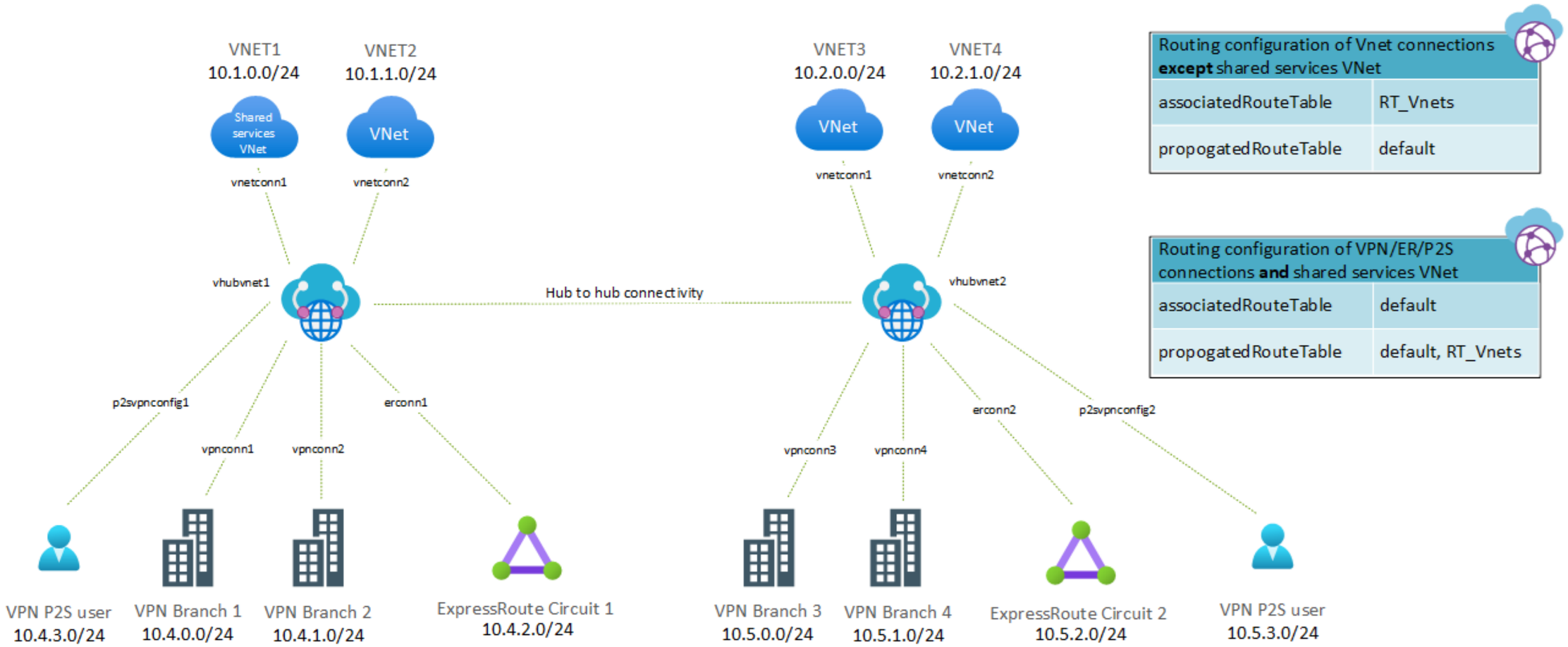
Hub-spoke topology with virtual WAN consists of:

- Hub VNet is a connection point for a number of 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 or ExpressRoute gateway
- Secured Virtual Hub
- Spoke Virtual Networks
- VPN device
- Virtual WAN hub
- Gateway Subnet
- 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

Assisted Practice

Creating a Vnet

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been tasked with recommending a network provisioning solution. Azure resources should be able to securely connect with one another, the internet, and on-premises networks using the solution.

Assisted Practice: Guidelines

Steps to create a Vnet are:

1. Login to your Azure portal
2. Create a virtual network
3. Select Virtual network
4. Select Resource group
5. Create Vnet

Unassisted Practice

Creating a Subnet

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been tasked with recommending a network addressing solution.

Unassisted Practice: Guidelines

Steps to create a subnet are:

1. Login to your Azure portal
2. Navigate to the virtual networks dashboard
3. Create a Subnet

Unassisted Practice

Creating a Public IP Address

Duration: 10 Min.

Problem Statement:

Demonstrate a networking solution that allows inbound Internet traffic to communicate with Azure resources and vice versa.

Unassisted Practice: Guidelines

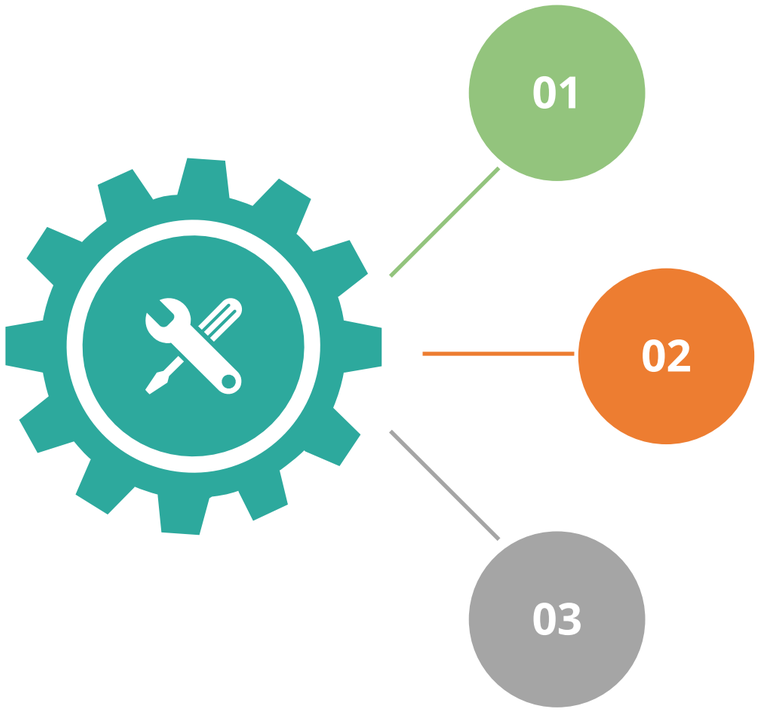
Steps to create a public IP address are:

1. Login to your Azure portal
2. Create a resource
3. Search the Marketplace box
4. Create the Public IP address

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 your own 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-prem computer and service name from VMs or role instances in Azure	Customer-managed DNS	FQDN only
Azure hostnames from on-prem 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 or 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.

- For full-featured DNS, use Azure DNS private zones or customer-managed DNS servers
- 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.

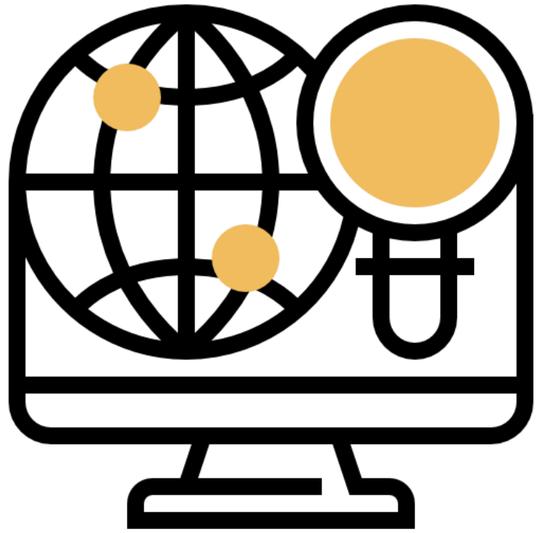
Azure-Provided Name Resolution

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

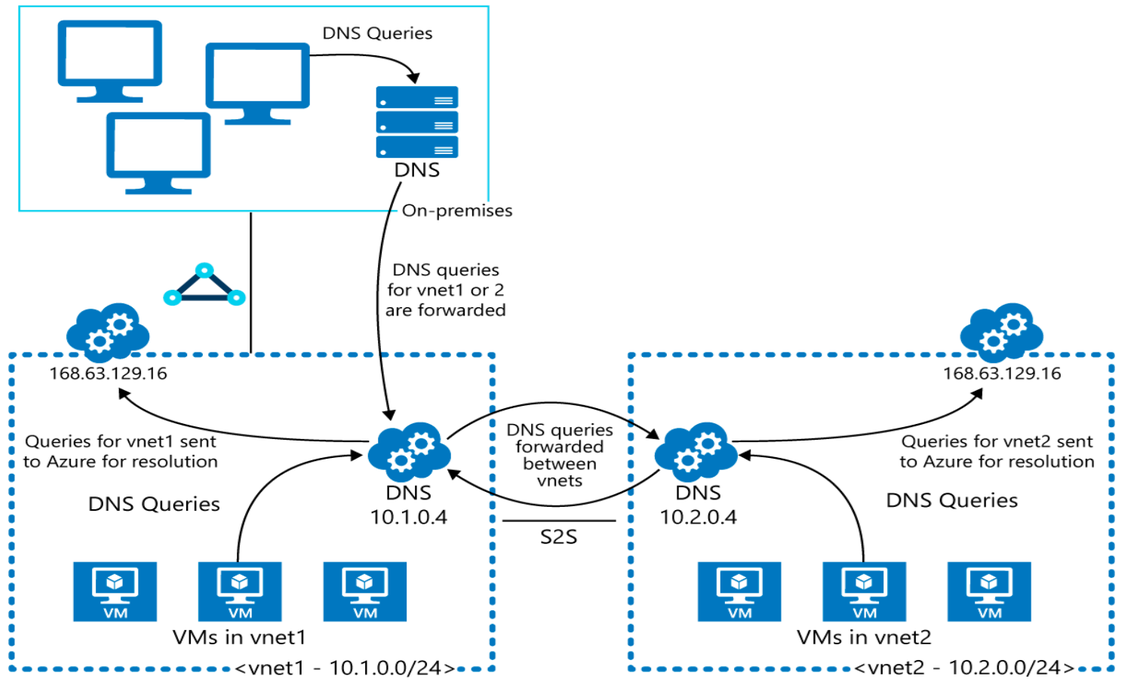
Name Resolution Using Customer-Provided DNS Server

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



Name Resolution Using Customer-Provided DNS Server

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

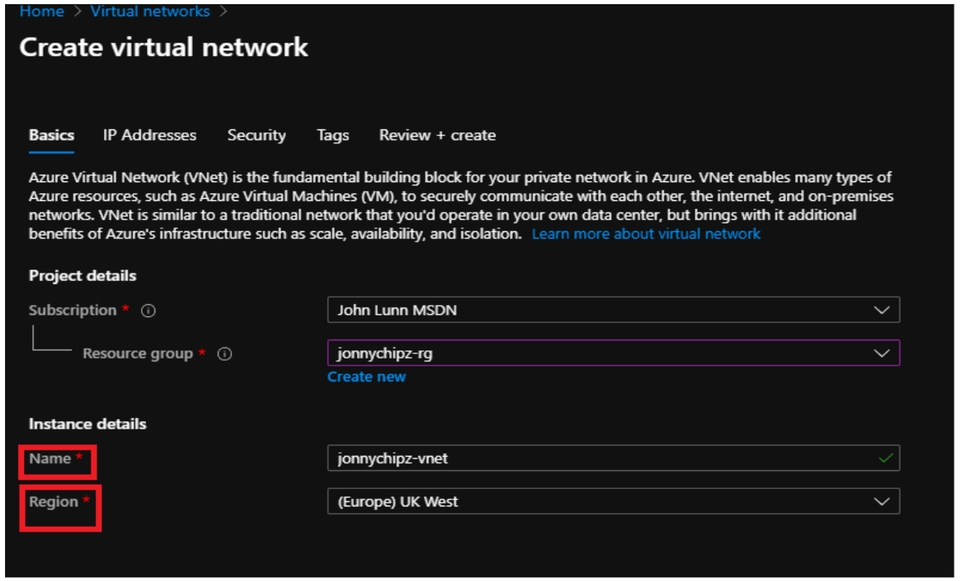


Use conditional forwarding rules to send DNS queries to the correct virtual network for resolution as each virtual network's DNS suffix is different.

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 is where all Azure resources are produced. Only a virtual network in the same region can be used to create a resource.

Segmentation

These are the segmentation considerations:

- The user can construct many virtual networks per subscription and per 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 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

These are the best practices for Virtual Network:

- Ensure non-overlapping address space
- Ensure that the entire VNet address space is not covered
- Configure a few larger VNets rather than many small ones, this prevents management overhead.
- Secure VNets by assigning Network Security Groups to subnets

Network Security Solution Recommendation

Network Security

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

Secures traffic flow amongst applications

Secures traffic flow between applications and the internet

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.

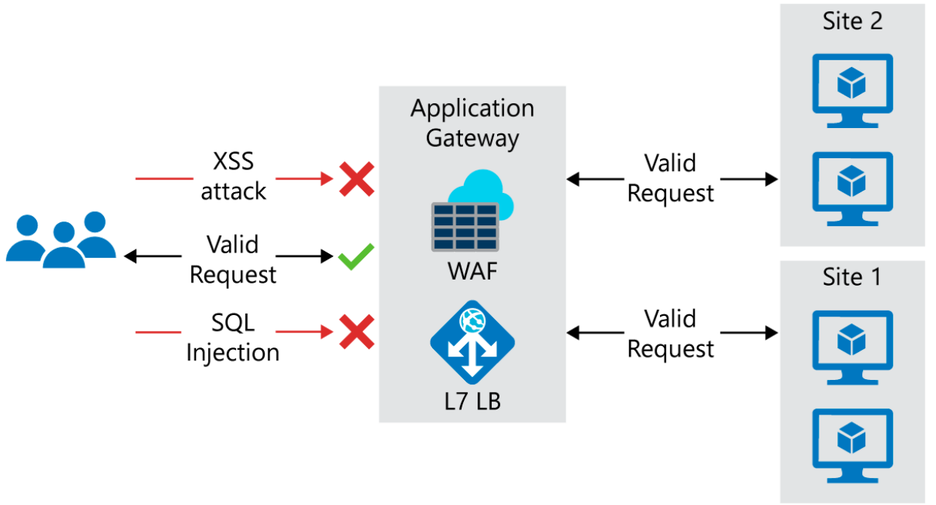
Border Gateway Protocol (BGP) routes

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 ExpressRoute connection.

Internet Protection

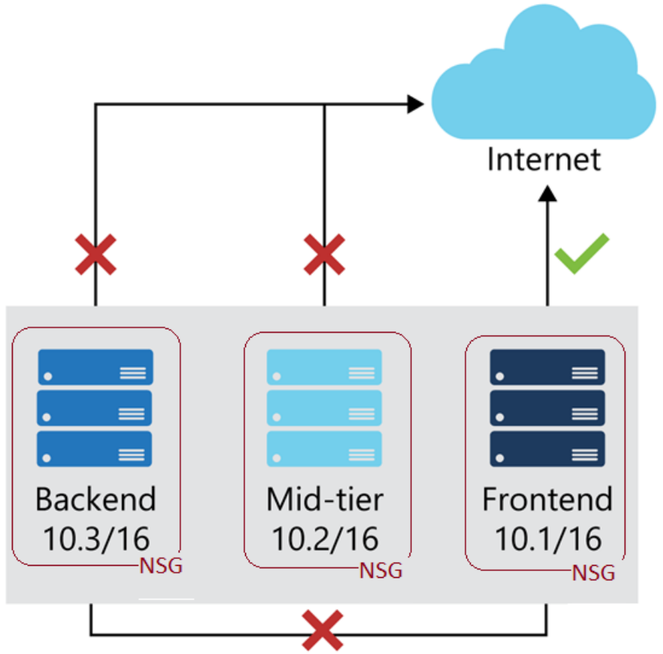
Different ways of restricting traffic from internet:

- 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.

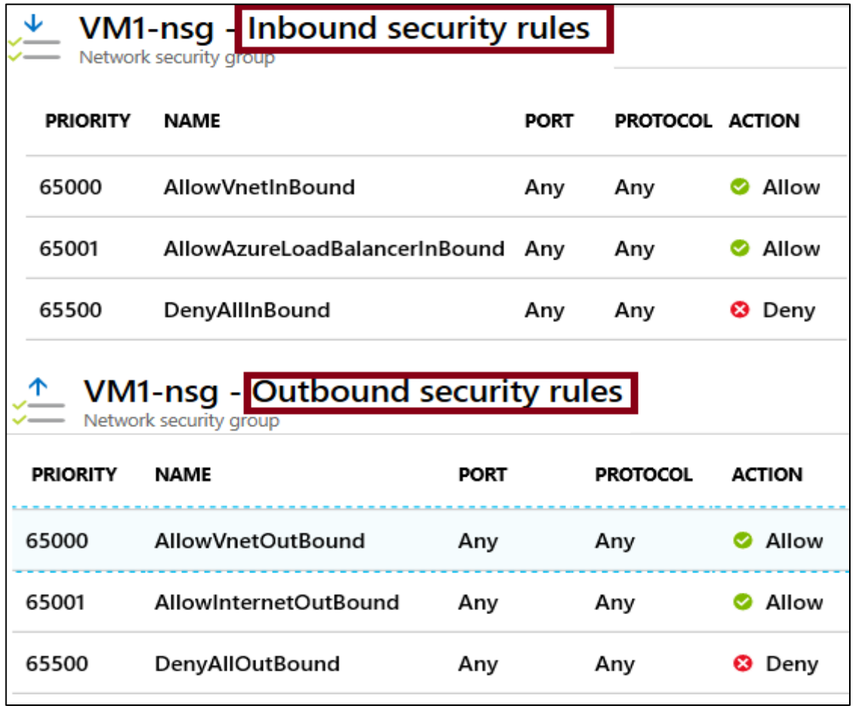
Network Security Group (NSG)

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

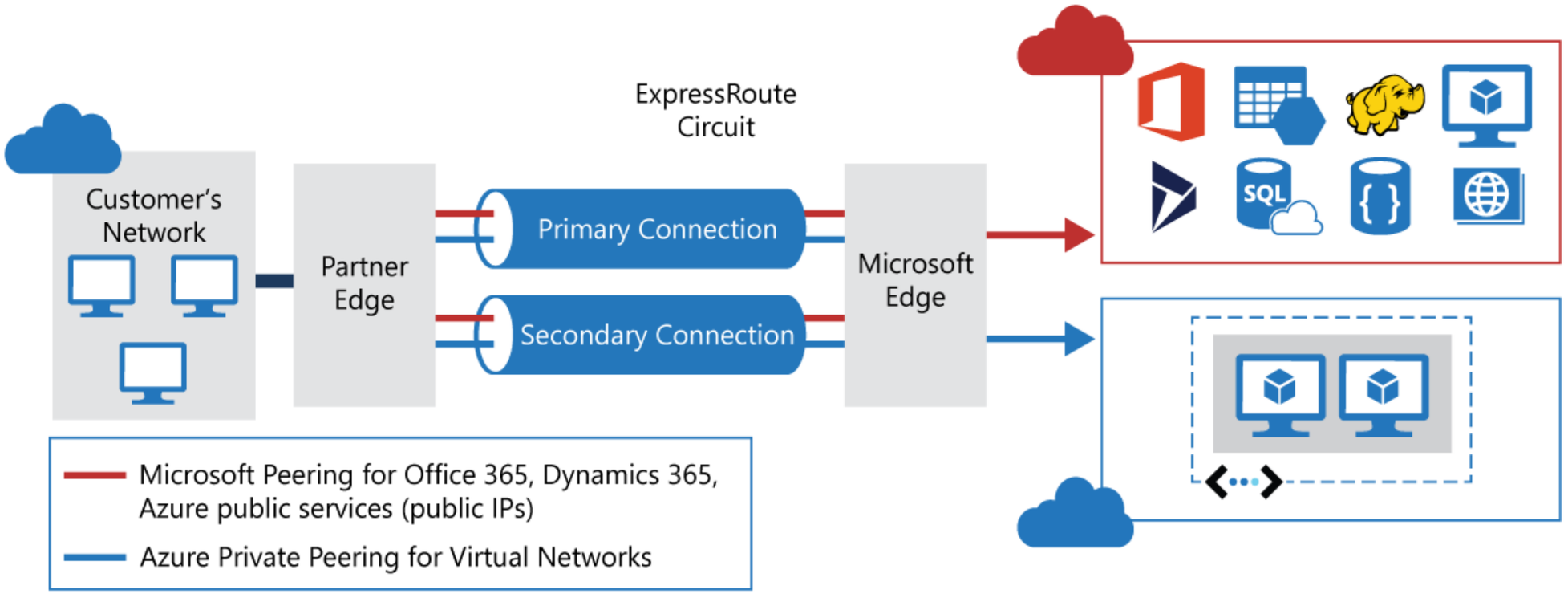
Network security group

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.



Unassisted Practice

Creating an NIC

Duration: 10 Min.

Problem Statement:

Demonstrate how to use an Azure network solution to connect an Azure Virtual Machine to the internet, Azure, and on-premises resources.

Unassisted Practice: Guidelines

Steps to create an NIC are:

1. Login to your Azure portal
2. Create two virtual networks
3. Peer Virtual Networks

Assisted Practice

Creating an NSG

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been asked to provide your organization with an Azure solution that can be used to activate a rule or access control list (ACL) that allows or denies network traffic to virtual machine instances on a virtual network.

Assisted Practice: Guidelines

Steps to create an NSG are:

1. Login to your Azure portal
2. Create a resource
3. Search Marketplace box
4. Create the Network security group

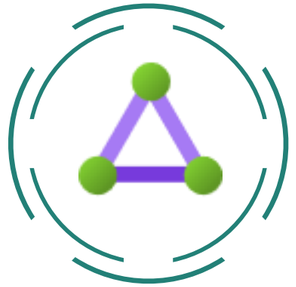
Network Connectivity Solution Recommendation

Virtual Network Connectivity

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

Vnet Peering

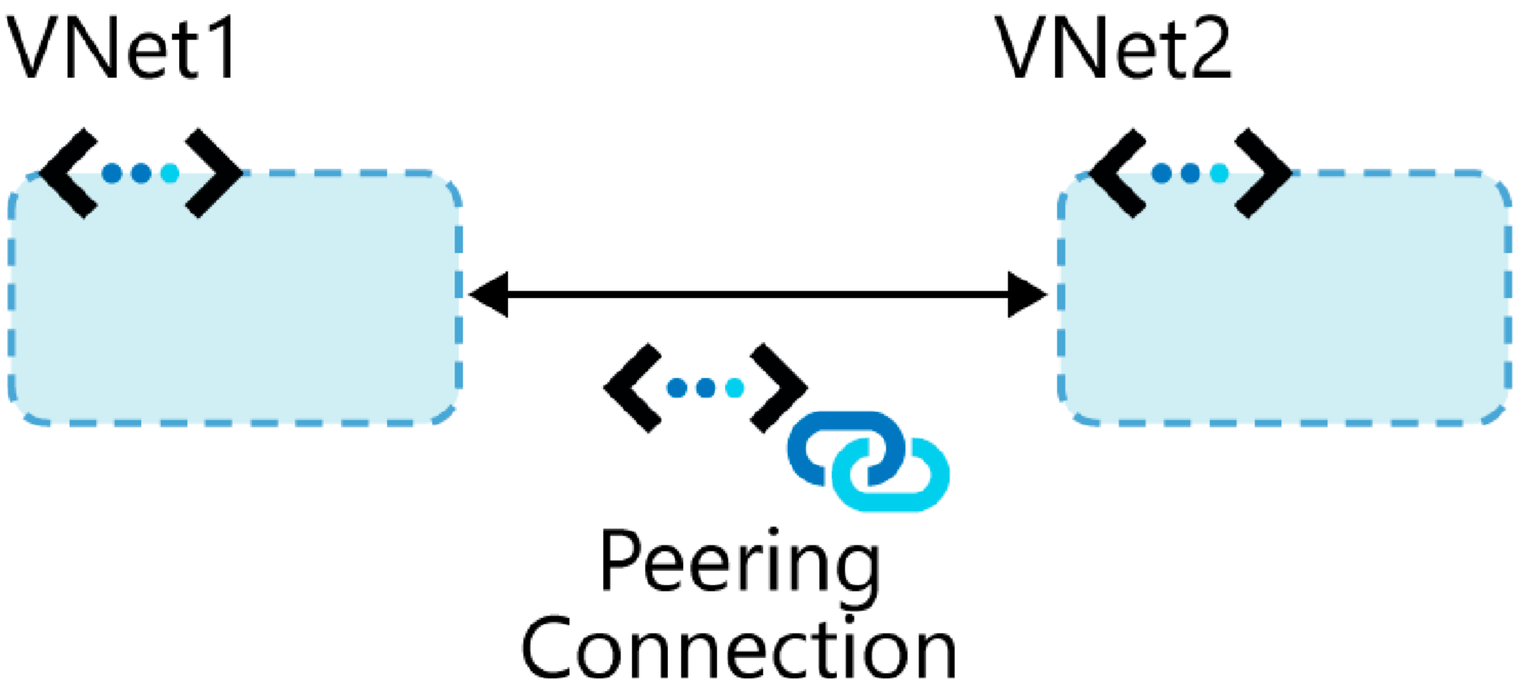
VPN Gateway Connections



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

When it comes to VNet Peering, keep the following in mind:

Reciprocal connections:

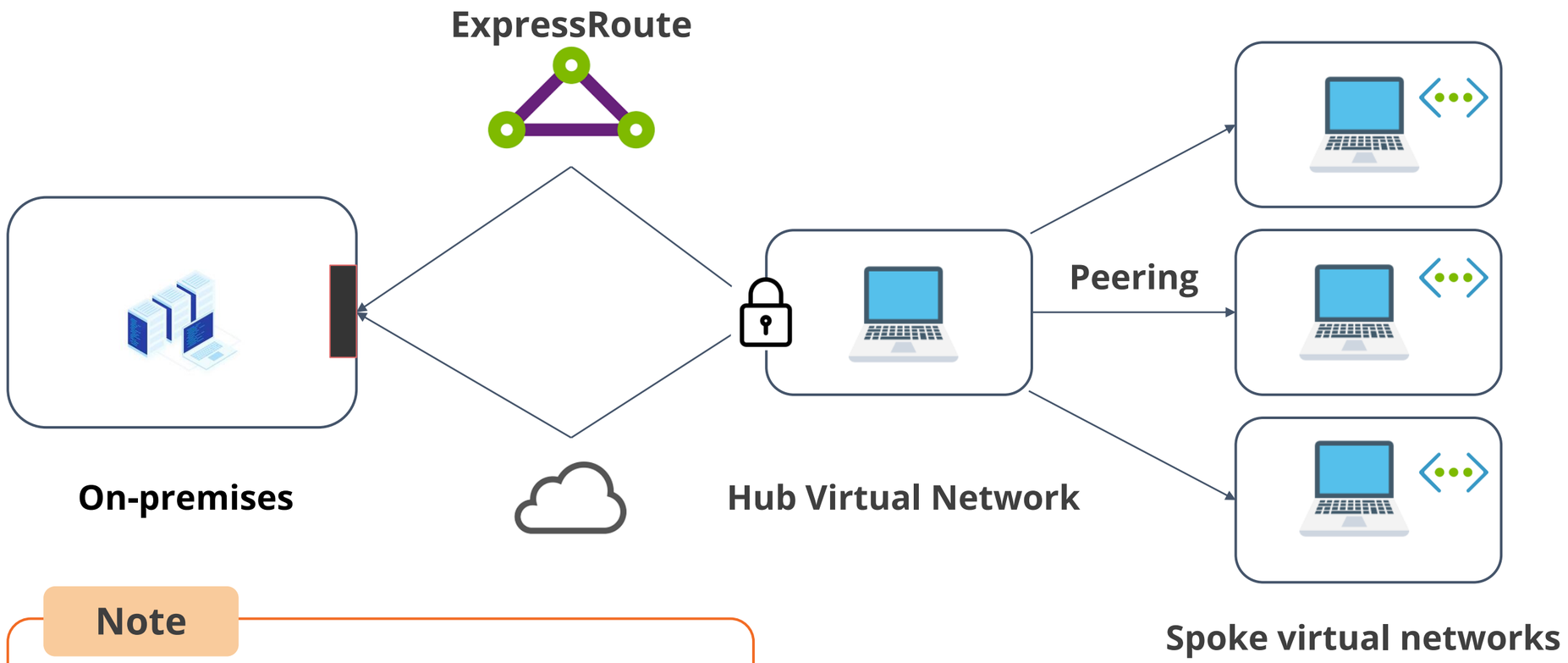
A user must establish a connection on each virtual network to link the networks while using virtual network peering.

Cross-subscription connections:

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

Transitivity

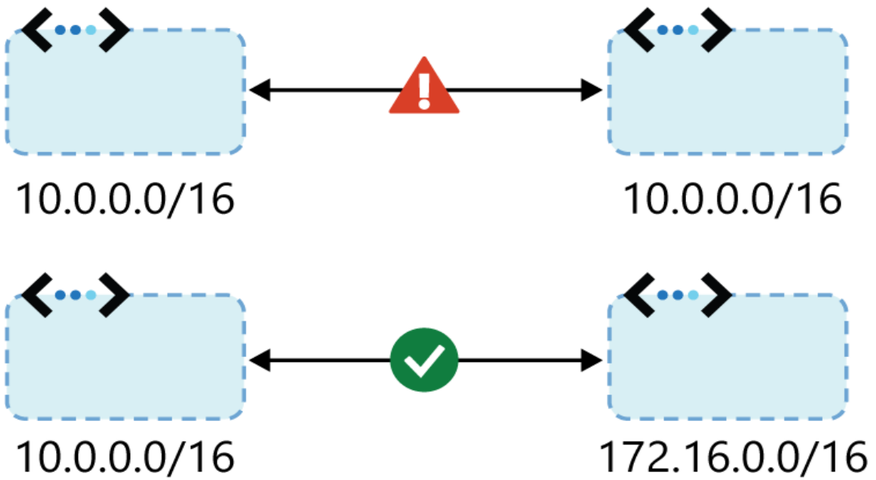
Peer-to-peer transitive routing is a concept used in Azure to describe network traffic that is routed via an intermediary virtual network between two virtual networks.



Note

Virtual network peering is nontransitive.

Gateway Transit



Benefits

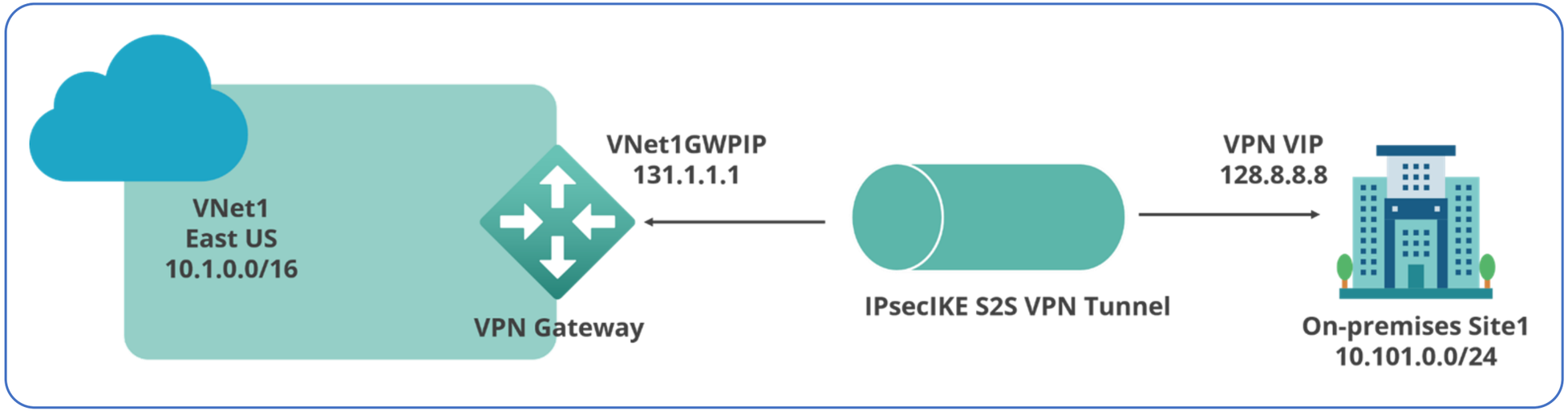
- Facilitate cross-premise connectivity
- Enable the allow gateway transit option in the hub
- Enable the use remote gateway option on the spoke

Peering considerations

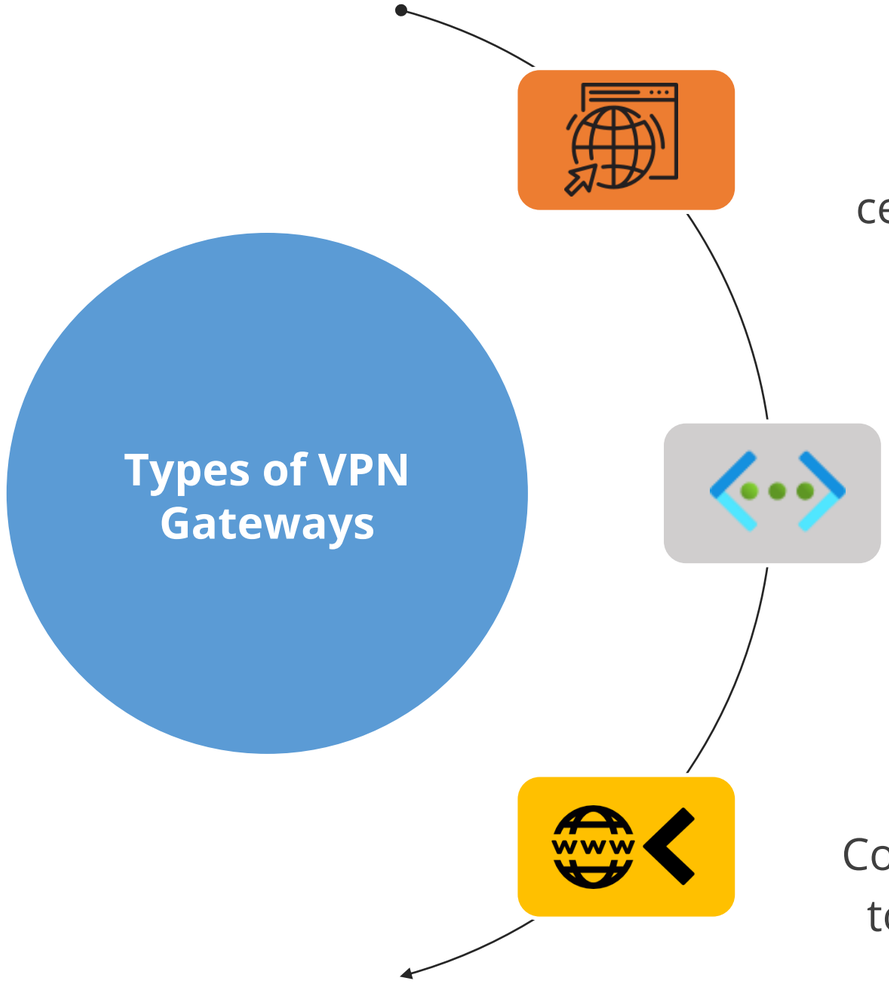
- IP address spaces should not overlap
- Peering is the recommended option

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

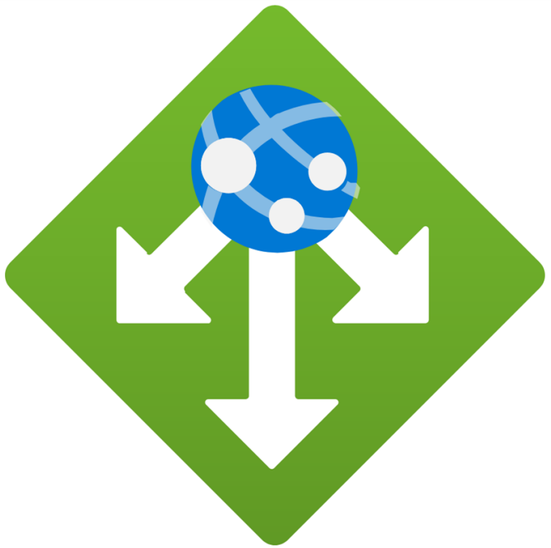
VNet Peering Versus VPN Gateways

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

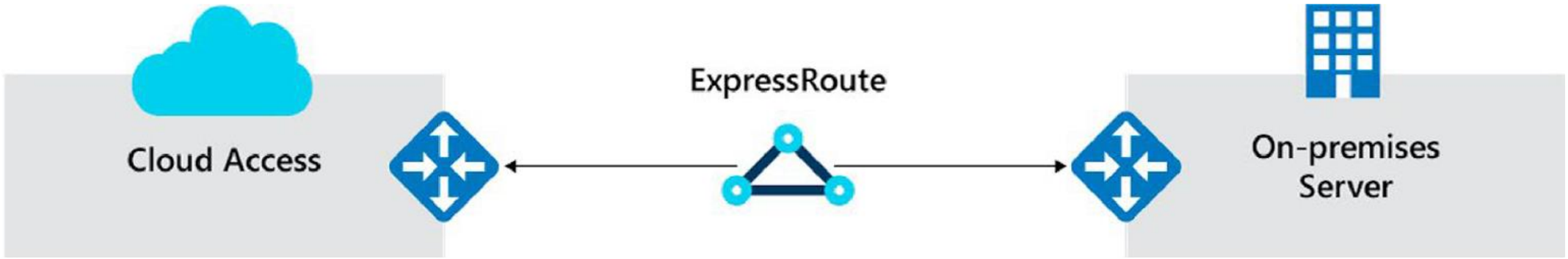
Virtual Network peering and VPN gateways support connecting:

- 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.

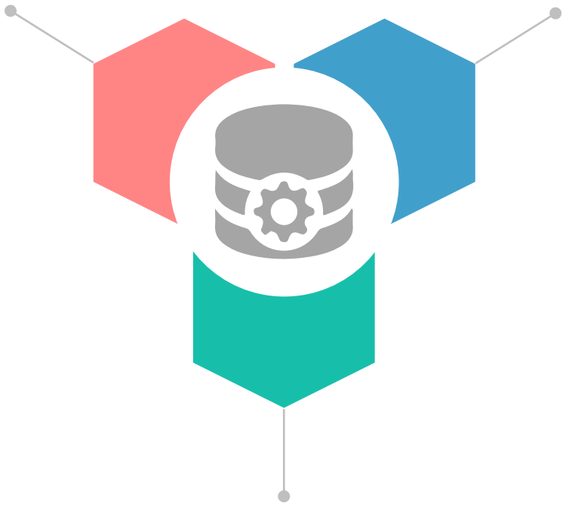
Benefits

- It configures traffic management and routing in ExpressRoute using circuits
- Supports multiple circuits across various regions
- Supports connections using various connectivity providers
- 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

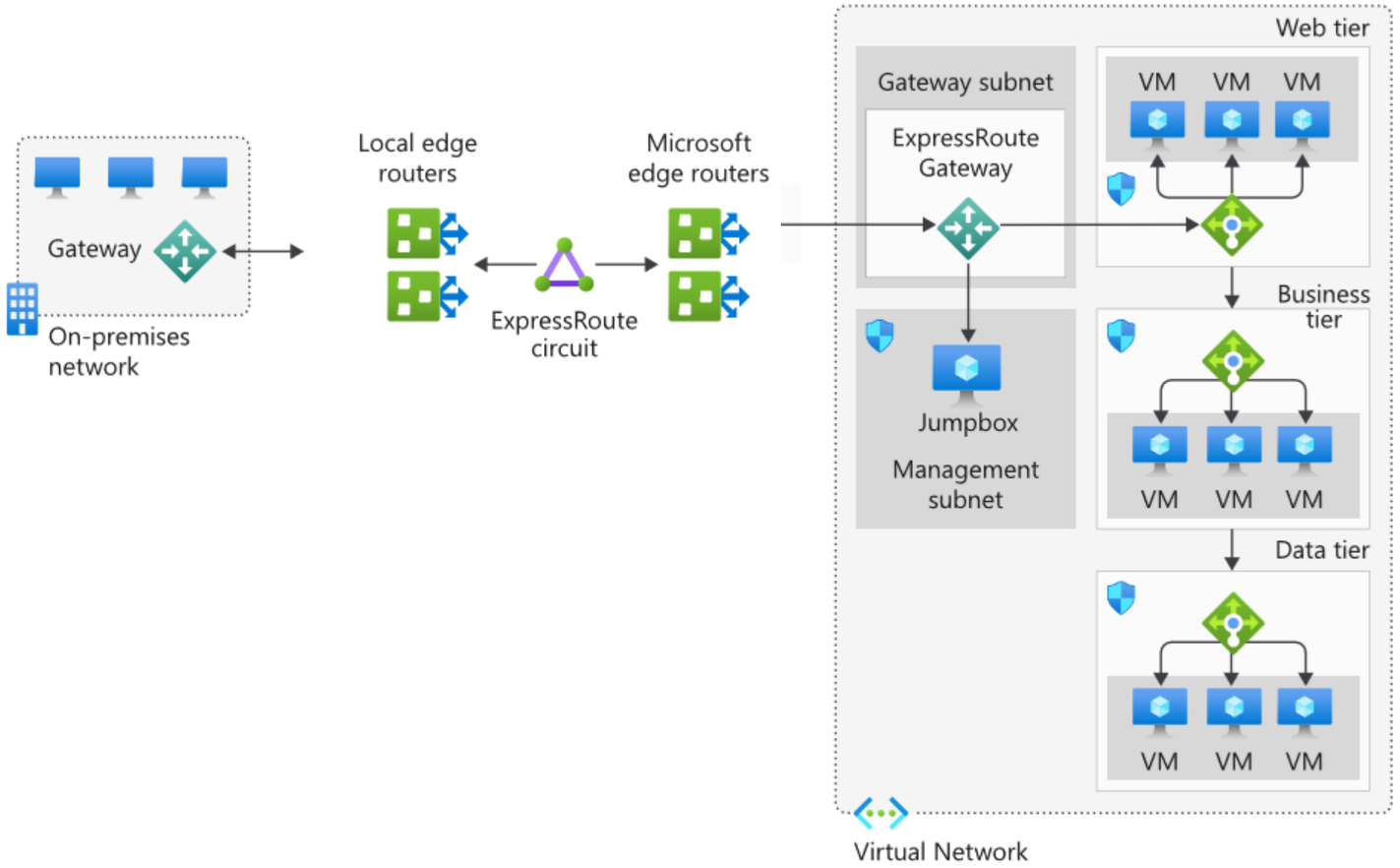
- Have as many circuits as the user needs to match bandwidth requirements

Microsoft Peering

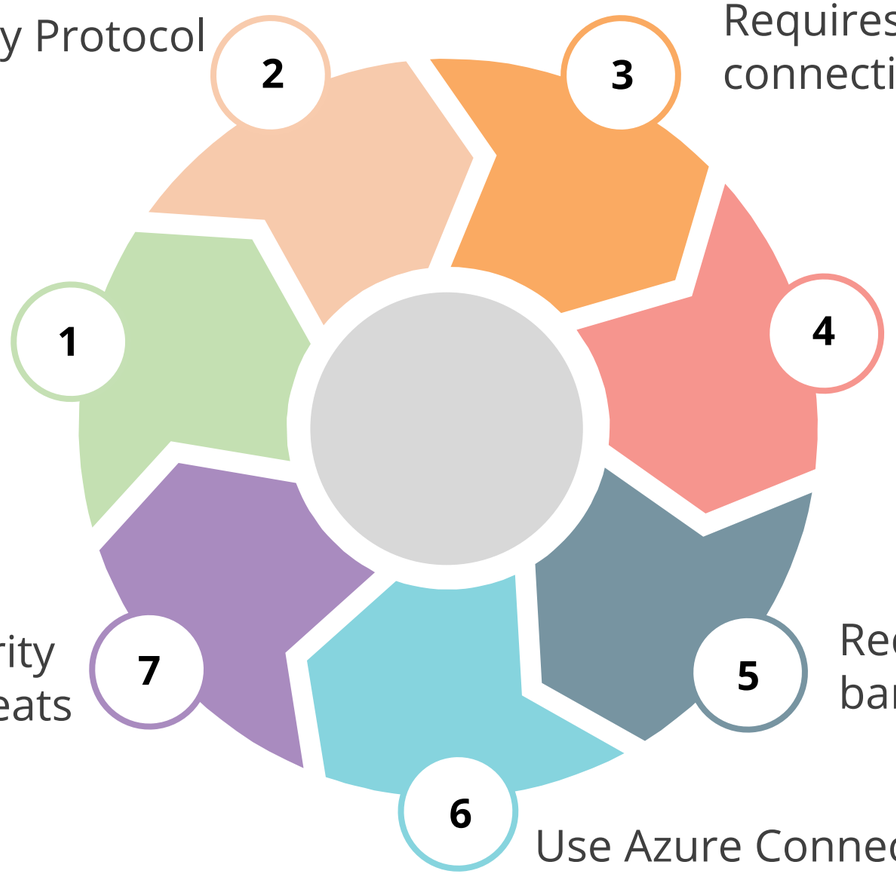
- Provides connectivity to all Microsoft online services
- Requires a public IP address

ExpressRoute Reference Architecture

The following figure shows the architecture of how ExpressRoute works:



ExpressRoute Considerations



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

Assisted Practice

Vnet Peering

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been asked to assist your organization with an Azure network solution that can help your organization seamlessly connect two or more Virtual Networks in Azure.

Assisted Practice: Guidelines

Steps to create a VPN Gateway are:

1. Login to your Azure portal
2. Create two virtual networks
3. Peer the virtual networks

Assisted Practice

VPN Gateway

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been asked to assist your organization with an Azure network solution that can be utilized to deliver encrypted traffic over the public Internet between an Azure virtual network and an on-premises site.

Assisted Practice: Guidelines

Steps to create a VPN Gateway are:

1. Login to your Azure portal
2. Create a virtual network
3. Create a subnet configuration
4. Create the subnet configuration for the virtual network
5. Create the gateway subnet
6. Create subnet configuration for the virtual network
7. Create a VPN gateway

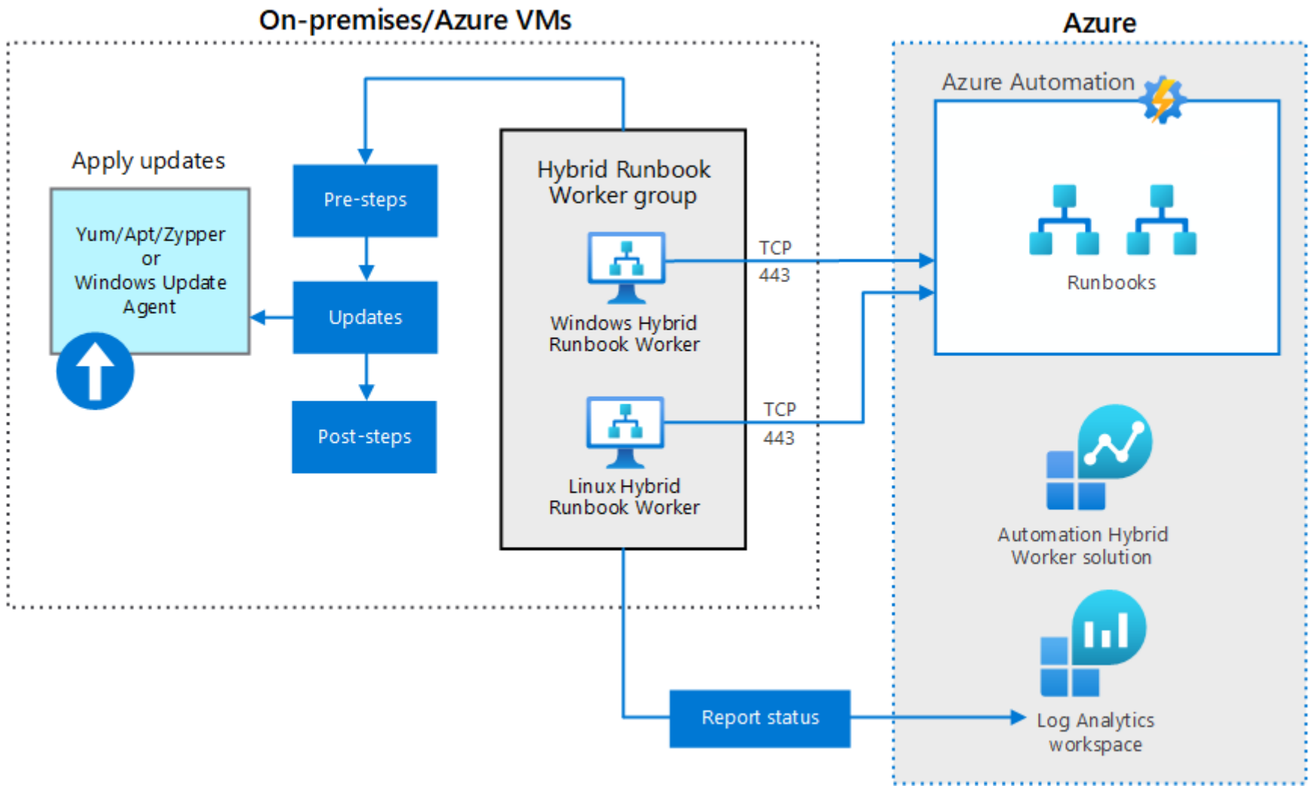
Automating Network Management Solution Recommendations

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

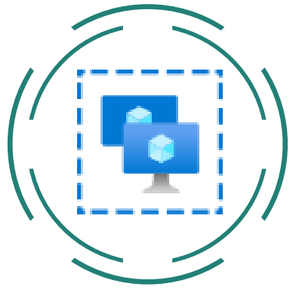
The Hybrid Update Management architecture is used for:

- 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

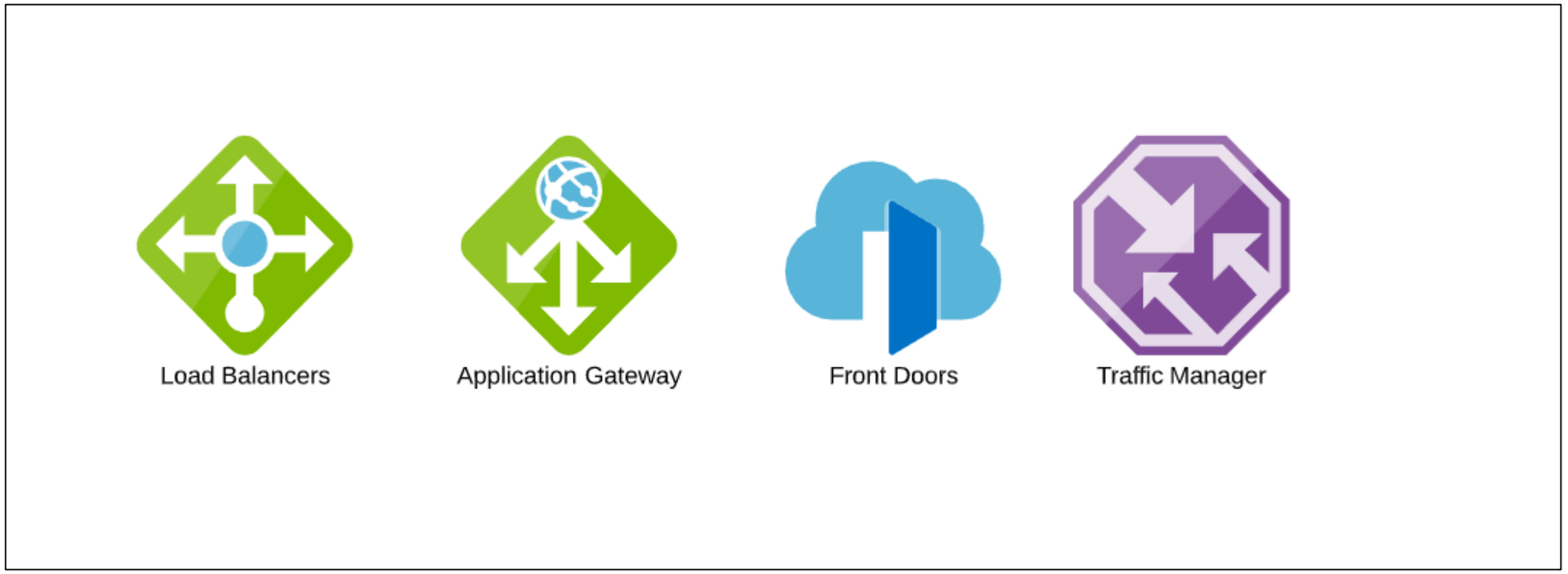


Availability Considerations

Recommend Solution for Load Balancing and Traffic Routing

Load Balancing and Traffic Routing

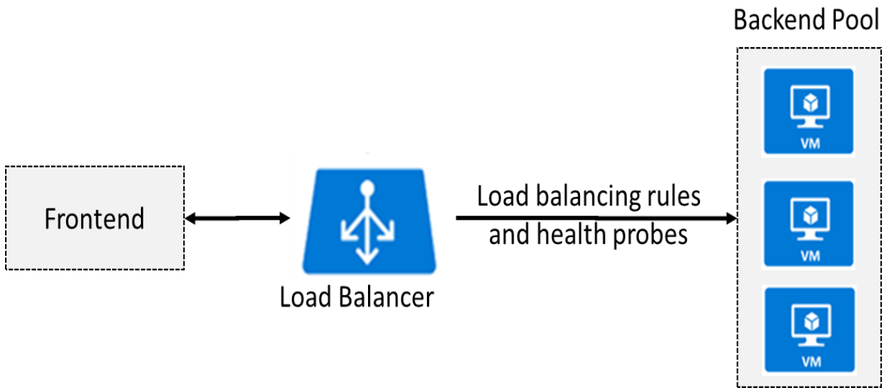
Azure offers these services for managing network traffic distribution and load balancing:



Depending on the user's demands, these services can be used individually or combine the ways to create the best solution.

Azure Load Balancer

Load Balancer distributes inbound traffic to backend resources



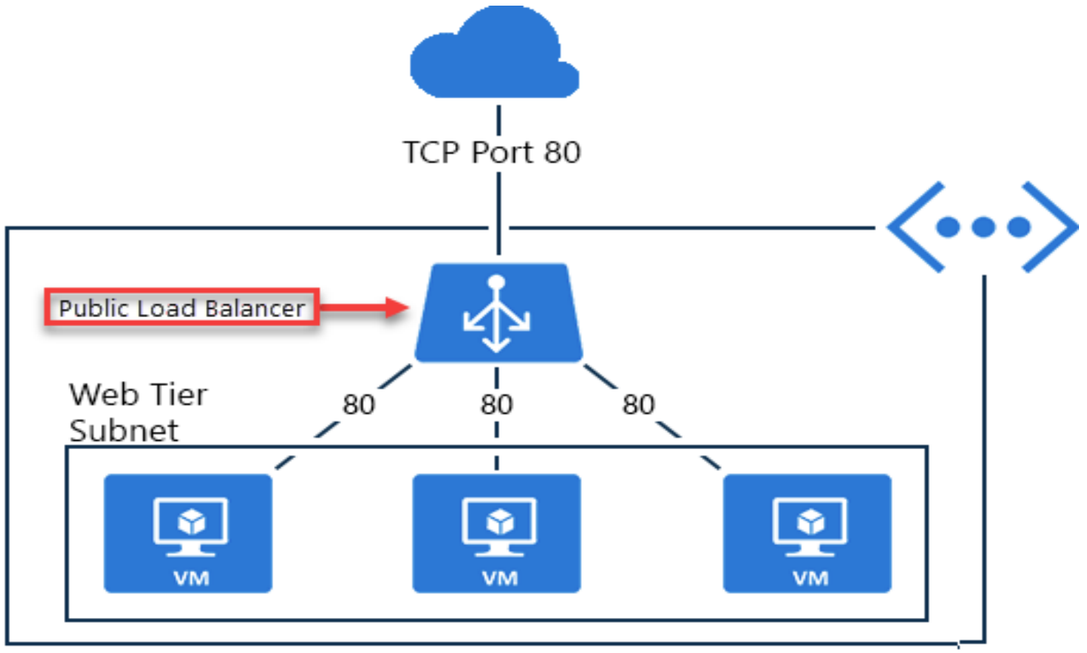
The on-premises web applications are protected with secure remote access

Azure Load Balancer

Azure Load Balancer is of two types:

Public Load Balancer

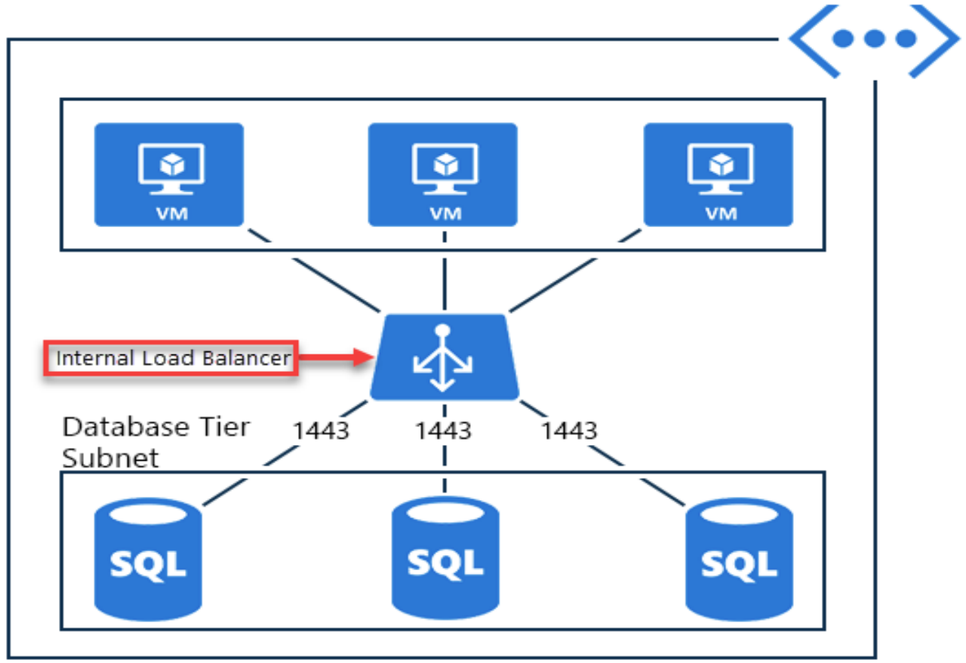
Maps public IP addresses and port number of incoming traffic to the VM's private IP address and port number and vice versa.



Applies load balancing rules to distribute traffic across VMs or services

Internal Load Balancer

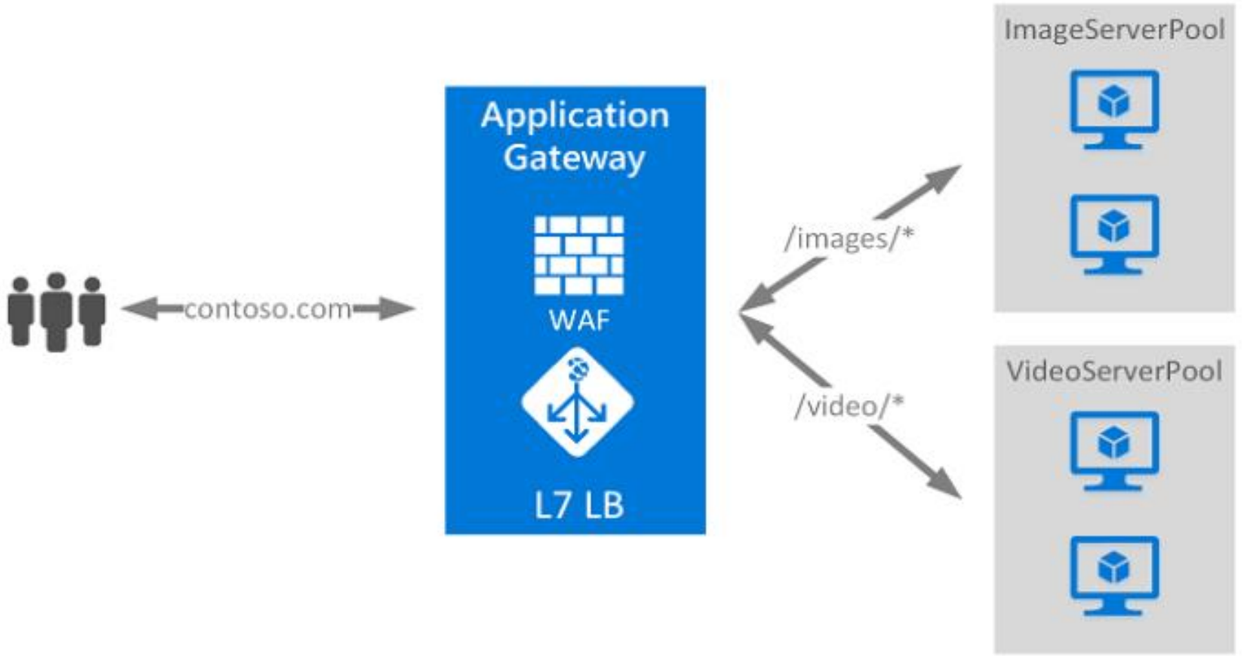
Directs traffic only to resources inside a virtual network or those which use a VPN to access Azure infrastructure



Enables load balancing within a virtual network, for cross-premises virtual networks, multi-tier applications, line-of-business applications

Application Gateway

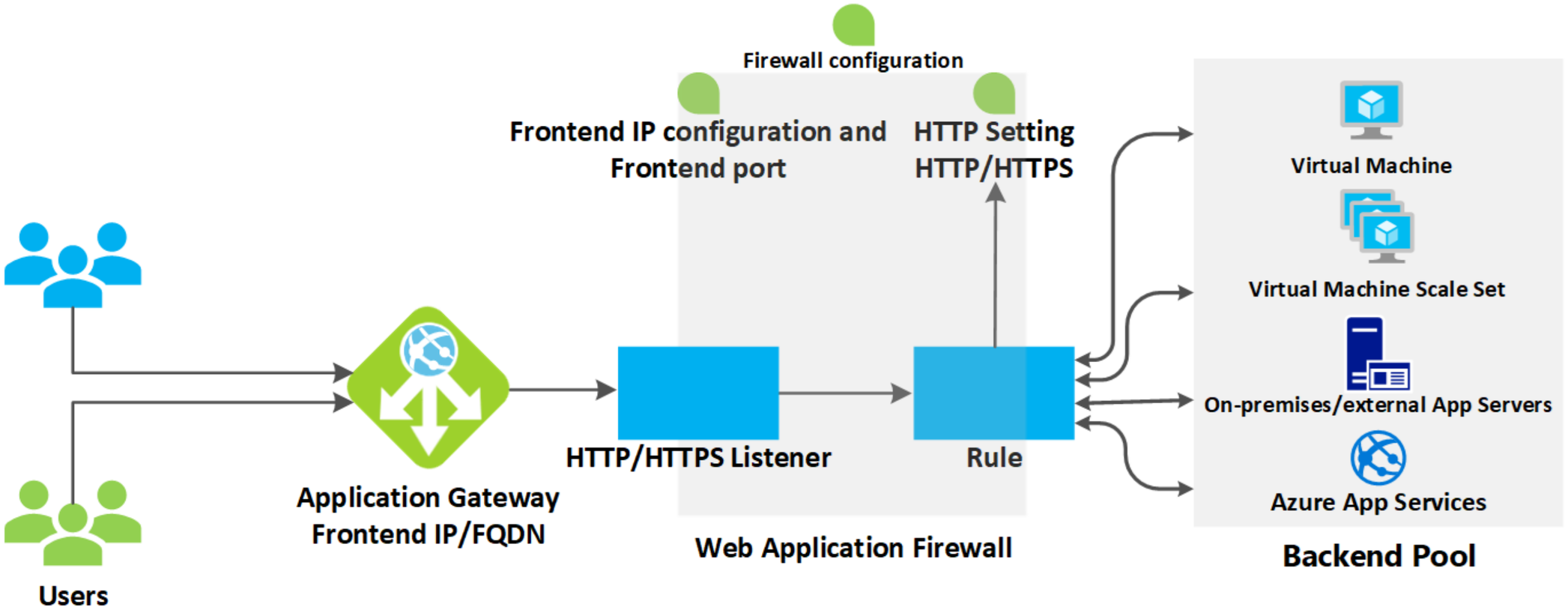
It controls the queries that clients can make to a web application.



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

Application Gateway

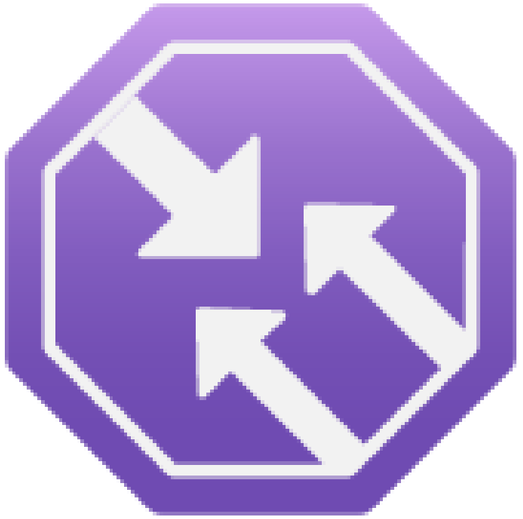
The workflow of Application Gateway is shown below:



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 our apps are highly available and highly scalable.

Traffic Manager

These are the features of a traffic manager:

- Increase application availability
- Improve application performance
- Distribute traffic for complex deployments
- Service maintenance without downtime
- Combine 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
10 Min.

Duration:

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 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 Application Gateway
4. Create an Application Gateway

Assisted Practice

Traffic Manager

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been asked to assist your company with an Azure Network solution that uses DNS to route client requests to the right service endpoint using a traffic-routing approach.

Assisted Practice: Guidelines

Steps to create traffic manager workspace are:

1. Login to your Azure portal
2. Create a resource
3. Create a Traffic Manager profile
4. View the Traffic Manager profile

Assisted Practice

Azure Front Door Service
Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been asked to provide your company with an Azure Network 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.

Assisted Practice: Guidelines

Steps to create an Azure Front Door are:

1. Login to your Azure portal
2. Create a resource
3. Search for Front Door in the search box
4. Configure Azure Front Door

Key Takeaways

- Application Gateway manages requests and routes traffic to a pool of web servers.
- Traffic Manager is a network service used to route users to web app endpoints in potentially different data centers located around the world.
- Network security is protecting 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

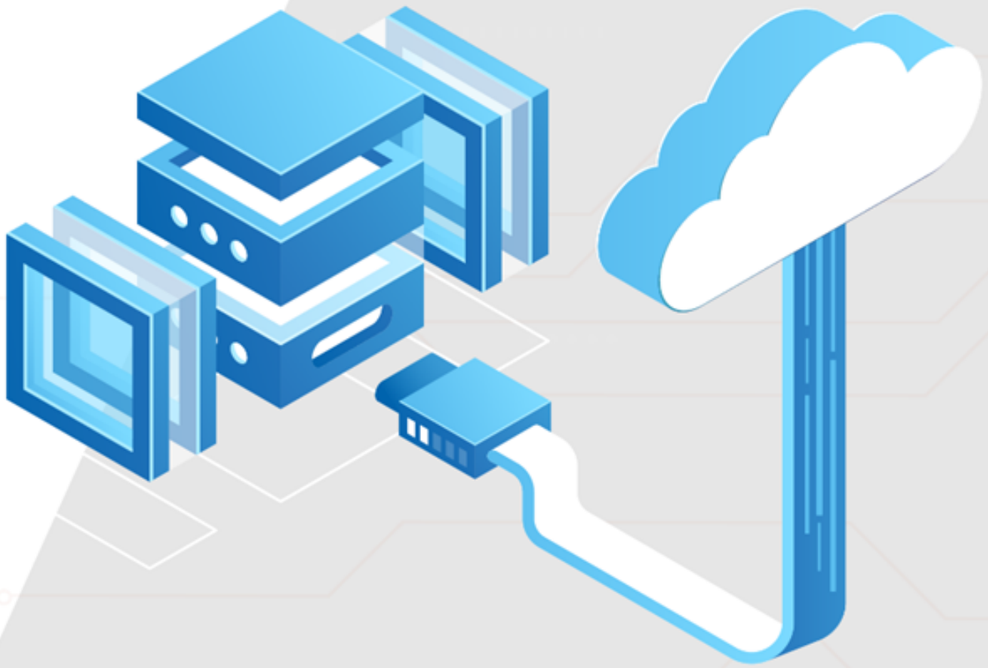
Objective: You are working as a Principal Engineer in an organization, and you have been asked to design a solution for an on-premise network to deploy a virtual appliance. The plan is to deploy multiple Azure VMs and connect the on-premises network to Azure using a site-to-site connection.

You need to also 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