**Configure and manage virtual networks for Azure administrators**

Azure Virtual Networking

* Infrastructure as a server resource
* Platform as a service to communicate with the internet
* Vnets allow for segmentation and isolation when implementing multiple virtual networks
* Similar capabilities to networks on-premises

Communicate between azure resources

* Virtual networks; used to connect to other resources such as vms, app service, Kubernetes, vm scale sets
* Service endpoints; connect to azure resources such as sql databases and storage accounts

Communicate with on-premises

* Point to point vpns;
* Site to site vpns; links on premises vpn device to azure vpn gateway in a virtual network. This can appear as a local network and is connected via internet
* Azure expressroute; for environments with large bandwidth and higher levels of security

Route network traffic

* Route tables; defines how traffic should be directed.
* Border gateway protocol; works with azure vpn gateway to propagate bgp routes to azure vnets

Filter network traffic

* Network security group; resource that contains inbound and outbound rules to allow or block traffic based on factors such as source and destination ip
* Network virtual appliances; specialized app like a vm used to run functions such as running a firewall or WAN optimization

Virtual network

* Link virtual networks together called ‘peering’

VPN Gateway

* A specific type of gateway that can be an encrypted endpoint connection. It can send encrypted traffic between azure vnets over ms’s dedicated network that links azure datacentres in different regions.
* Each vnet can only have one VPN gateway.

VPN gateways

* Network-to-network
* Cross premises IPsec VPN tunnelling
* Point-to-point connections

Plan a VPN gateway

* Point 2 point over the internet
* Site to site over the internet
* Site to site over a dedicated network, like azure expressroute

VPN gateway

* Route based; uses any-to-any traffic selectors.
* Policy based; typically built on firewall devices that performs packet filtering. Combination of prefixes from both networks to define how traffic is encrypted/decrypted through IPsec tunnels

**Design an IP addressing schema for your azure deployment**

Azure IP addressing

* Azure use private ip addresses. Range is the same as on-premises ip addressing
* Typical network design consists of vnets, subnets, network security groups, firewalls, and load balancers
* No routers or switches used in azure.
* Subnets isolate front end services like web servers, dns, and back-end services like databases and storage systems
* Network security groups filters internal and external traffic at the network layer
* Firewall has more capabilities for filtering and app layer filtering.
* Azure combines both security group and firewall for a more secure isolation of resources

Non routable ip addresses

* 10.0.0.0 to 10.255.255.255
* 172.16.0.0 to 172.31.255.255
* 192.168.0.1 to 192.168.255.255

Public IP

* Dynamic; dynamic is automatically assigned and can vary during the lifespan of the resource. When you create a vm an ip is assigned to when you stop a vm then its released again.
* Static; ips that will not change over time, can set the allocation method to static, ip address is only released when you delete the resource
* Basic; assigned using dynamic or static. Can be assigned to any resource that can be assigned a public IP such as VPN gateway, app gateway, internet facing load balancers
* Standard; secure by default and closed to inbound traffic. Must specifically allow by using network security group

Public IP prefix

* Cannot bring your own public ip used on your on-prem location. An ip is assigned from a pool of available resources but you can set your ip prefix to ensure a static ip range.
* Advantage of prefix is that you can specify firewall rules based on that prefix knowing that they will not change

Private Ip Addresses, used for comms within vnet

* Dynamic; assigned through DHCP and varies over lifespan
* Static; DHCP assigned and does not change unless deleted

Private Ips available are

* 10.0.0.0/8
* 172.16.0.0/12
* 192.168.0.0/16

**Virtual Network Peering**

* Vnet regional peering; connects vnets in the same region, like two networks in the south island region
* Global vnet peering; connected to two different regions like north island and south island in new Zealand

Reciprocal connections

* When you connect one to another you’re not connecting them both unless its established from both ends

Cross subscription vnet peering

* When both networks are in different subscriptions. Cant really work unless both admins from each subscription grants peering on their vnet

Transitivity

* What this means is that vnets connects to each other like a>b>c>d and so forth. Meaning vnet A>D is impossible

Overlapping Ips

* Vnets cannot have overlapping ips otherwise they wont be able to communicate

**Secure and Isolate by using network security groups**

Network security group

* Filter network traffic to and from az resources in a vnet
* Assigning sec groups to s subnet instead of individual interfaces reduces admin and management. This ensures the subnets have consistent rules.
* When there are no NSG assigned then by default all traffic is allowed
* Inbould rules apply to traffic entering the NSG
* Outbound rules are to traffic leaving the NSG
* Default azure will set a inbound and outbound rules for you

Secure rules

* Name
* Priority; number between 100-4096,lower the number higher the priority
* Source and destination;
* Protocol; tcp, udp, or any
* Type; inbound/outbound
* Destination
* Port range;
* Access; allow/deny

Default rules

* Rules that cannot be changed but can be overruled

Inbound

|  |  |
| --- | --- |
| 65000 | Allow vnet inbound, everything within know ip space |
| 65001 | Allow internet outbound, load balancer |
| 65500 | Deny all outbound,denying everything else |

Outbound

|  |  |
| --- | --- |
| 65000 | Allow vnet inbound, |
| 65001 | Allow internet outbound, allow everything sent out to internet |
| 65500 | Deny all outbound, denying everything else |

Service tags

* Virtual network;
* Azure load balancer
* Internet
* Azure traffic manager
* Storage
* SQL

App security groups

* Allows for network security config for apps

Virtual Network service endpoints

* Endpoints are used to extend private addresses
* It allows to secure resources to only your virtual network
* Can connect to PaaS services directly to the private address to appear to be on the same vnet
* Available for services like azure sql, key vault, data lake, service bus, azure storage

**Connect VM via Azure Portal using Bastion**

* Intermediate harden instance you can use to connect to target server using SSH or RDP over TLS (transport layer security)
* Some devices cannot run rdp client like chromebook
* Helps protect against port scanning
* Can use service to monitor and manage remote connections
* Must be at least /27 or 32 addresses
* No need to config NSG to the Az bastion subnet.
* Bastion is deployed in a separate subnet called azure bastion subnet

Concurrent sessions

* Up to 25 rdp sessions
* Ssh connection sot 50

Roles needed for Azure Bastion

* Reader role on vm
* Reader role on NIC with private ip of vm
* Reader role on the az bastion resource

Why azure bastion?

* **Can simplify management of its VMs**

At what resource level or scope does an Azure Bastion connection apply to?

* **Virtual network or peered virtual networks**

You decide to deploy Azure Bastion to an existing virtual network by using the Azure CLI. What resources do you need to create?

* **Subnet named AzureBastionSubnet, public IP, and Azure Bastion**

Several of your peers are having trouble connecting to VMs by using Azure Bastion. What isn't likely to cause the problem?

* **The public IP address of the destination VM**

You want to add an extra layer of security to Azure Bastion. Where can you start?

* **Apply role-based access control (RBAC) and the least privilege to use and manage Azure Bastion**