**Configure and manage virtual networking**

**Implement and manage virtual networking**

**168.63.129.16** – Azure Wire service, reserved public IP for azure, DHCP, default gateway, DNS, VM Agent comm

Vnet – Virtual Network (10.10.0.0/16). All resources in same vNet can see each other

NIC is attached to VNet/Subnet then NIC is associated with VM – it has the TCP/IP configuration

Subnet – Inside the VNet (10.10.1.0/24)

NSG – is associated in VNet or Subnet or NIC. OSI Layer 4. Stateful firewall

Name resolution options  
 Default mode, azure-provided name resolution

azure provided, Single name resolution, cloudapp.net, No custom DNS names, functions only within Vnet even if you link Vnets.

Azure DNS – Hosted Service, to delegate public zone and private zone

Check TCP/IP settings

VM > Networking > Network Interface > IP Configurations

Setting VNet of VM can only be done during creation

This is where to set Private IP dynamic or static and Public IP associate or disassociate

**Configure Subnets**

Delegated subnets – injected services that has a reserved subnet label (AzureFirewallSubnet a reserve label, Azure Bastion, Application Gateway, etc)

**Service Endpoints –** Products that allows service endpoints, to allow connectivity to the subnet

Vnet > Service Endpoints > Add > Choose which resource/service (storage, blob, DB) > choose subnet

Configure storage > Firewalls and Virtual Networks > Allow only selected network > Choose Vnet > Choose Subnet > Firewall (add your client IP to allow)

**Private Endpoints –** Privatelink – incorporate resource to a subnet. Creates a NIC for the resource in the subnet

FQDN can be configured via Azure DNS

Private Link > Create > Choose RG > Choose resource > Target sub-resource > Choose Vnet and Subnet > Choose DNS zone

**Routing**

NIC > effective routes

UDR (User defined routes)

To Create:

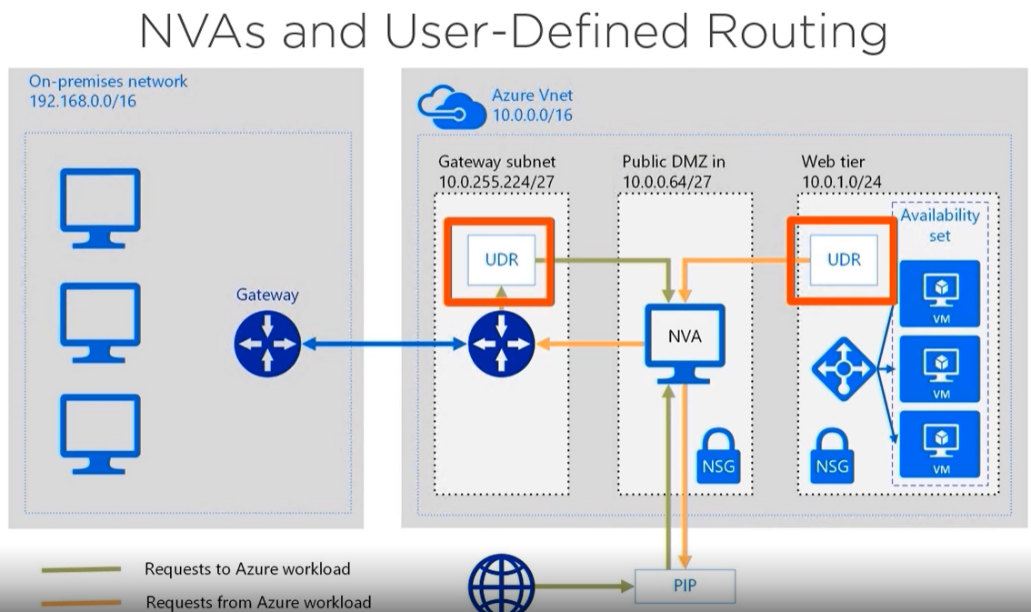
Route Tables > choose RG > name

To add routes:  
Route Tables > Choose the created route table > Routes > add > route name, address prefix, Next hope type

(type if NVA choose Virtual Appliance)

To associate:

Route table > Subnets > Associate > choose Vnet > Choose Subnet



**Peering –** To link Vnets. Creating Private routing path. You can make service chaining (hub and spoke, etc). Peering doesn’t support azure-provided name resolution.

Vnet > choose Vnet > Peerings > Add > Name of peering > configure if allow forwarded traffic

Not transitive routing (VNet1 and Vnet2 peered to VnetHub, Vnet1 cannot talk to Vnet2 by default) – to do this, you need to

-Create router in VnetHub (Network virtual appliance/router from Marketplace, or Microsoft Firewall, or VM)

-Deploy custom route tables – using route tables

**Secure access to virtual networks**

NSG and Security rules

NSG – stateful traffic filter, for inbound and outbound traffic.

OSI layer 4: Source and Destination IP address, Source and Destination port and Protocol

Security rules are evaluated in priority

Service Tags – Microsoft defined set of IP address prefixes aligned to azure services (SQL, etc)

Helpful for firewall rule management

Default Rules are not editable/deletable – just make a new rule that has higher prio

Associate NSG to subnet or Vnet

Create NSG > Define rules > Associate NSG to Vnet/Subnet

Evaluating security rules

Network watcher – There are tools available like,

Topology view

IP flow verify – traffic flow from to and which rule took effect

Effective security rules – see the effective NSG rules are effective on a resource

Connection troubleshoot

NVA – Network Virtual Appliance

3rd party network appliance – Cisco, Netapp

Azure Bastion – One bastion per VNet, Fully managed so no Stop and no RDP policy

Create:  
 Azure Bastion > Name > Subnet named AzureBastionSubnet > public IP address

Azure Firewall

Layer 3 to Layer 7

Create:  
 Firewalls > Add > add or use existing Vnet > create subnet named AzureFirewallSubnet > Public IP address

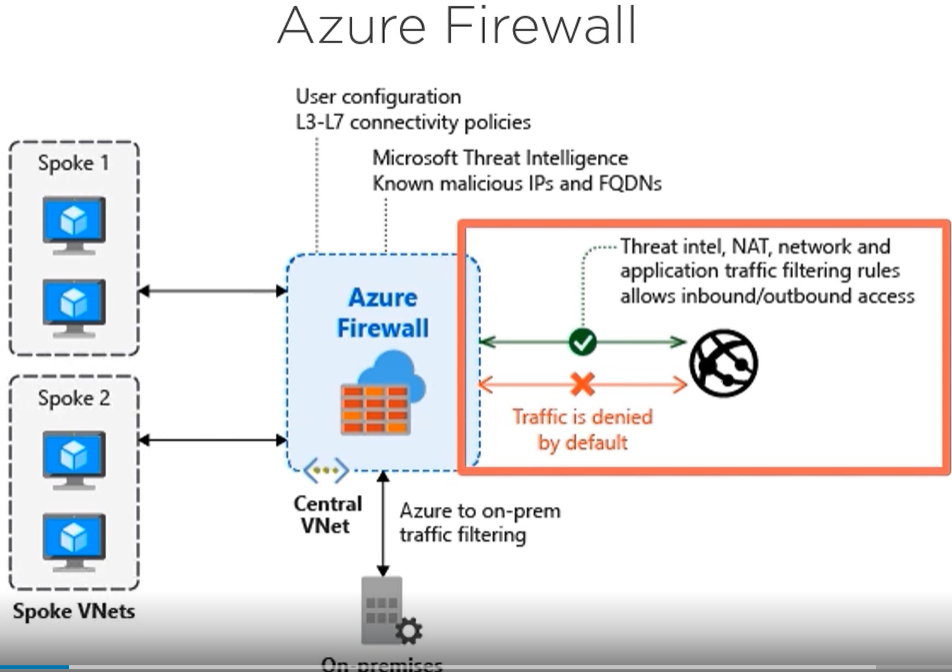
Then create a route table

Route tables > Add a route table  
 then in the created route table > routes > add a route > route name > address prefix > next hope type is virtual applicance > next hop address is the private IP of the Firewall >

Then go back to create route table > subnets > associate the Vnet and subnet that will use this route

To configure firewall rules – Firewalls > Rules

There is 3 rule collections – NAT rule collection, Network Rule collection and Application rule collection



**Configure load balancing**

General purpose LB, can be external or internal (if HTTP/HTTPS why not Application gateway?)

Use for HA for similar configured machines, Scalable performance, better service level

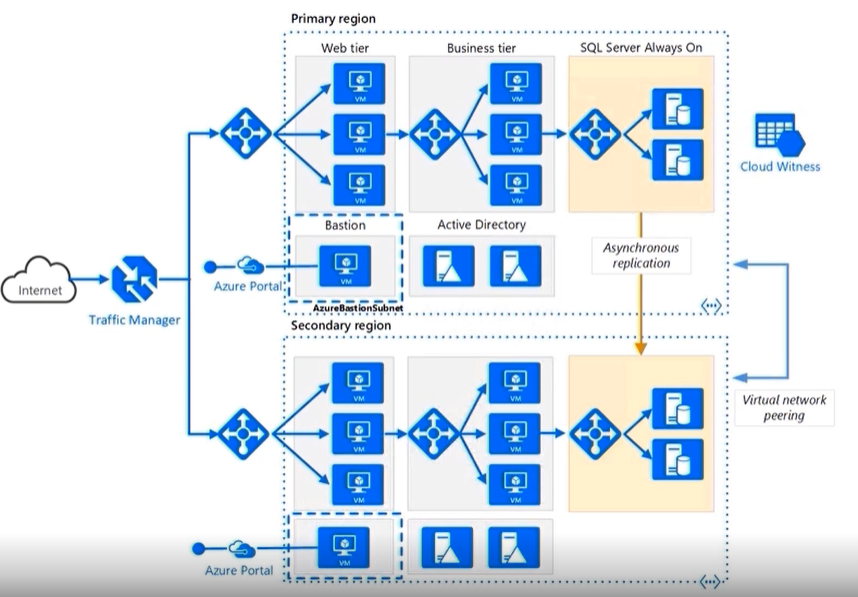
Components:

Front end configuration - Public ip address (multiple) (need Public IP address standard)

Hash based distribution – 5 tuple hash to figure how to distribution

Backend pool – identicaly configured VM’s

Health probe – to verify node is online (port check or HTTP probe)



Azure LB is regional only, so need to use TM for geo redundancy

Azure load balancer SKU

Basic: 300 backend instances, availability set or VMSS, not availability zone aware

Standard: 1000 backend instances, any VM on same Vnet, Availability zone aware

Sku cannot be changed, need to delete and redeploy again to change

Session affinity (NAT Rules)

Client IP affinity – to use RDP gateway (source IP stays the same, LB route to same host) Sticky

Client IP + protocol – for stateless workload, if IP or protocol change, the session is new, route new host

Floating IP / Direct Server Return

Use for backend SQL server pool. The return data bypasses the LB for faster response.

Troubleshooting LB

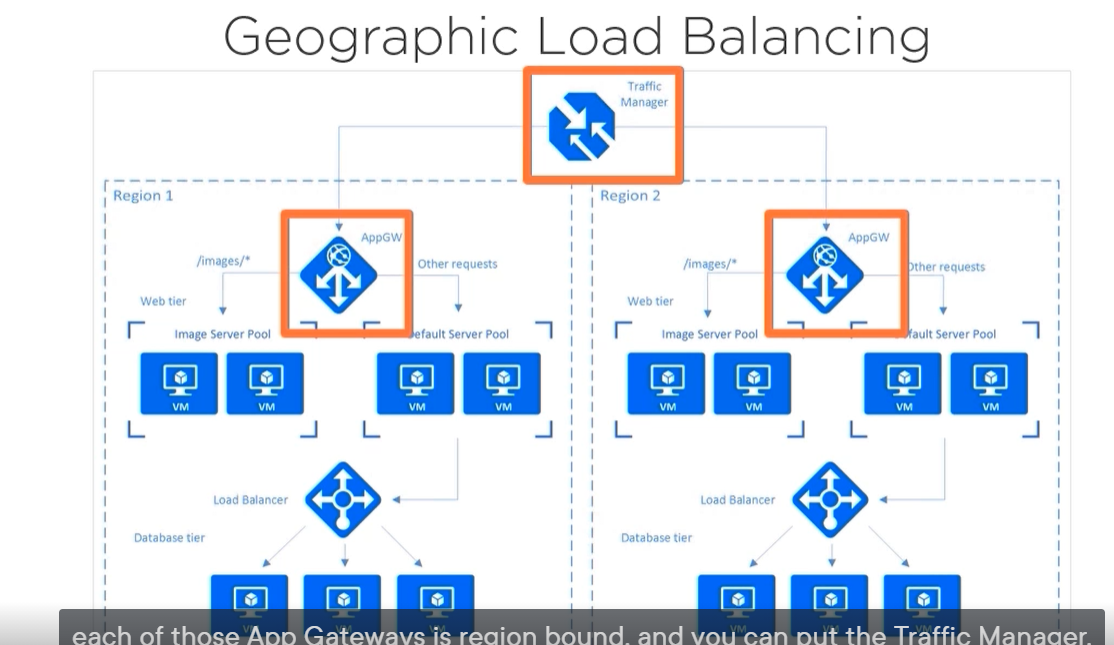
Tools: Service Health, Resource Health, Azure Monitor, PSPing, TCPing, Network watcher

Configure and troubleshoot Application gateway

Features:

OSI layer 7, HTTP(S) workloads only, pubic or private, WAF (Owasp)  
 SSL/TLS offload, AutoScale, Multi-site routing, Path-based routing

Components:  
 Frontend IP, Listener (for port, IP or cert), Rule, Backend pool, http setting, Custom probe



Creating Application Gateway:  
 Make sure NSG allows load balancer traffic > Create subnet for AppGateway > create app gateway > firewall status and mode (detection vs prevention – only for OWASP) > select VNet and Subnet > select if Front type (private, public or both) and add PIP if public > Backend tab for adding the backend pool > Configuration tab for adding routing rules (configure listener then backend targets rules).

Web application Firewall rules (WAF)

Azure service that can be associated to different appgateway

**Monitor and troubleshoot virtual networking**

Inspecting Virtual network traffic

Tools:  
 Network Watcher

Topology generator (GUI), track connection reachability, IP flow verify, Next hop (verify routing path), Effective security rules, VPN troubleshoot (deep logging of Azure VPN gateway), Packet Capture (gather ethernet frames and analyze with wireshark), Connection Troubleshoot (check direct TCP connection).

NPM – network performance monitor

Dependent on Log Analytics (Azure Monitor Logs)

Tools:

Performance monitor – monitor packet loss and latency

Service Connectivity monitor – Monitor any TCP endpoint (API’s, Saas, Paas applications, O365)

Express Route monitor – Bandwidth utilization

Log analytics Workspace

Aggregates all logs into a central workspace

Sources can be from VM, on prem or AWS/GCP (must have agents installed)

Data will be stored on a virtual database

Can be queried with KQL

Presented on Insights, Dashboard, PowerBI, etc

Log Analytics gateway is like a jumpserver that can send the logs to Workspace for airgapped infra

Hybrid cloud network traffic

Log analytics workspace > Solutions > NetworkMonitoring > Network performance monitor

Azure VPN gateway diagnostics log alerts

Create action like ITSM, Azure PowerApps, etc

Network Watcher VPN troubleshoot – wizard like troubleshooter

Network Watcher packet capture – download and open in Wireshark,etc

**Integrate an on-premises network with an Azure virtual network**

2 types of Azure VPN:

1. A. Site to Site VPN (S2S) – Always ON VPN using IPSec and IKE protocols

routing methods: Policy based (static) or Route based (dynamic)

Active-active or Active-passive HA

Reserved gateway subnet name = GatewaySubnet

B. VNET to VNET VPN – secure connection between Vnet, IPSec and IKE. Used to be used when peering is not yet available

Only used so that there is isolation or administrative limitation

Components: Virtual Network Gateway, Local Network gateway, Connections

1. Point to Site VPN (P2S) – Devices like routers, laptops, mobile phones, connects to the VPN

Supports OpenVPN, SSTP, IKEv2,

Authentication: Certificate based, Azure AD, RADIUS

Components: VPN Gateway, Server certificate, Client certificate, VPN client

To deploy Site to Site / Vnet to Vnet:

Create the GatewaySubnet  
Go to VNet > create GatewaySubnet

Create the Virtual Network gateway (VPN)

Go to Virtual Networks gateways > Add > choose Gatewy type: VPN or ExpressRoute> Choose VPN type: Route based or Policy based > choose SKU > Choose Vnet (automatically selects the GatewaySubnet created above > specify PIP

Create the Local network gateway (representation of the local network)

Go to Local Network gateways > Add > IP address or FQDN of the local network > specify address space

Add Connection

Go to the Created virtual network gateway > Connections > Add > choose between Vnet to Vnet / Site to Site or ExpressRoute > choose the Virtual Network Gateway > Choose the Local network gateway > provide Shared Key (PSK)

To deploy Point to site:  
Create the Virtual Network Gateway (same as above)

Go to the created Virtual Network Gateway > Point to site configuration> Specify address pool that is outside the Vnet > Tunnel type (SSTP, IKE, etc) > choose authentication (azure cert, radius, Azure AD) > download VPN client > install the client > Go to Windows VPN Settings