# Network ACL

 Network ACLs can be attached to subnets. By defualt every vpc wil have a default NACL which allows all incoming and all outgoing

 Network ACL act on

 priority (lower the number higher the priority)  action (allow/deny)

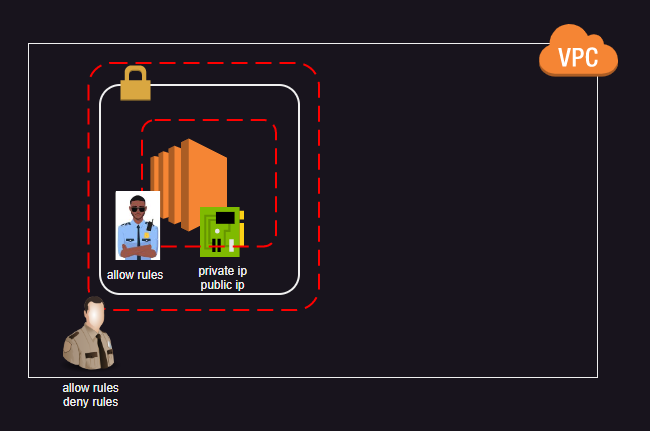
 protocol  port

 ip range (incoming/outgoing)  [Refer Here](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html) for official docs

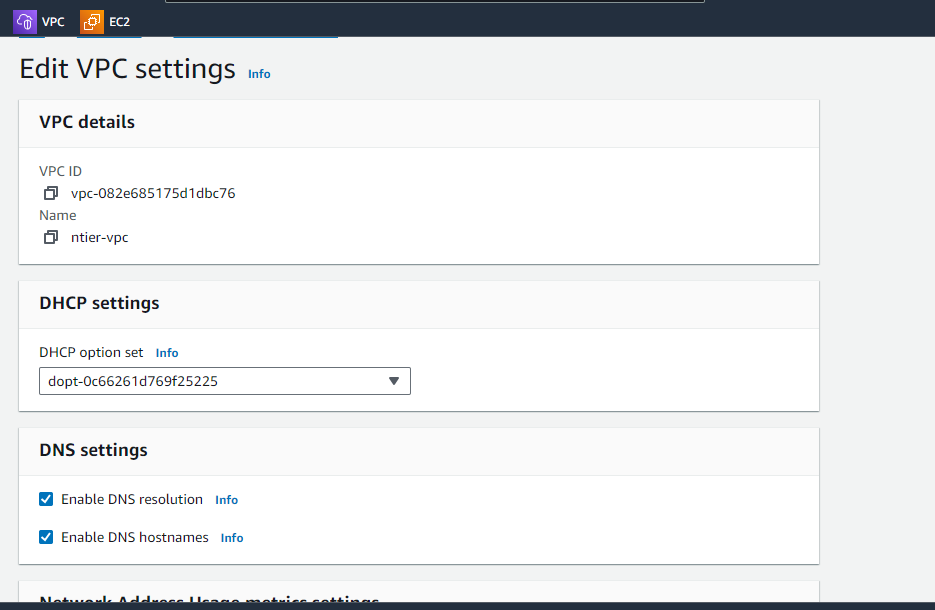
 Lets create an ec2 with the security group rules to allow

 ssh from my ip (client ip)  http from anywhere

 ping from anywhere

 Lets create an NACL, attach to the subnet which allows all tcp from anywhere  Allow all outbound in NACL

Enabling Public DNS Names in vpcs



# Azure Virtual Networks

 [Refer Here](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview) for official docs

 [Refer Here](https://learn.microsoft.com/en-us/azure/virtual-network/quick-create-portal) for creating virtual network  Steps:

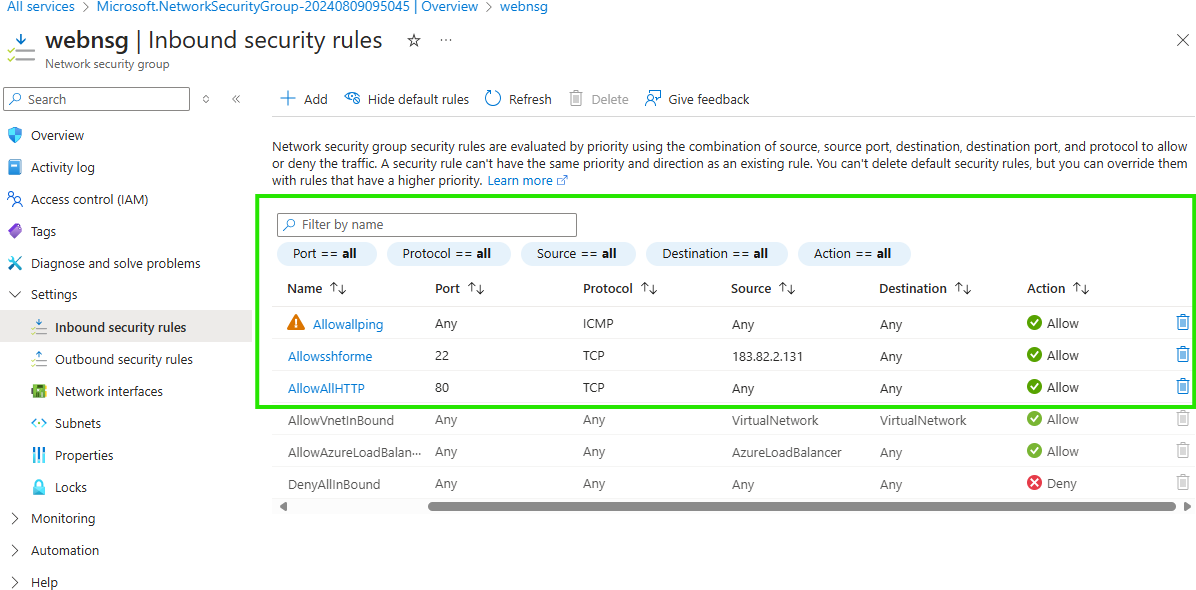
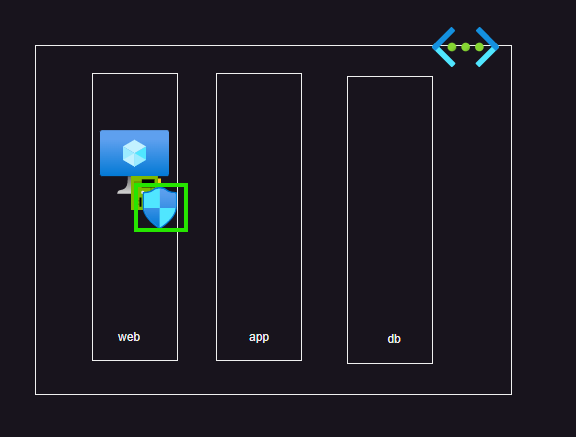
Create one or use existing resource group

 Create vnet with subnets

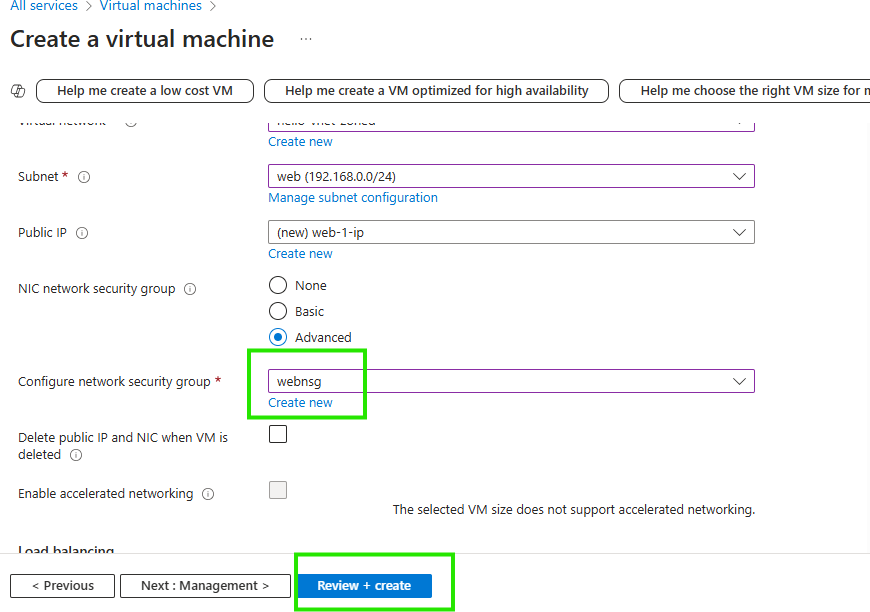
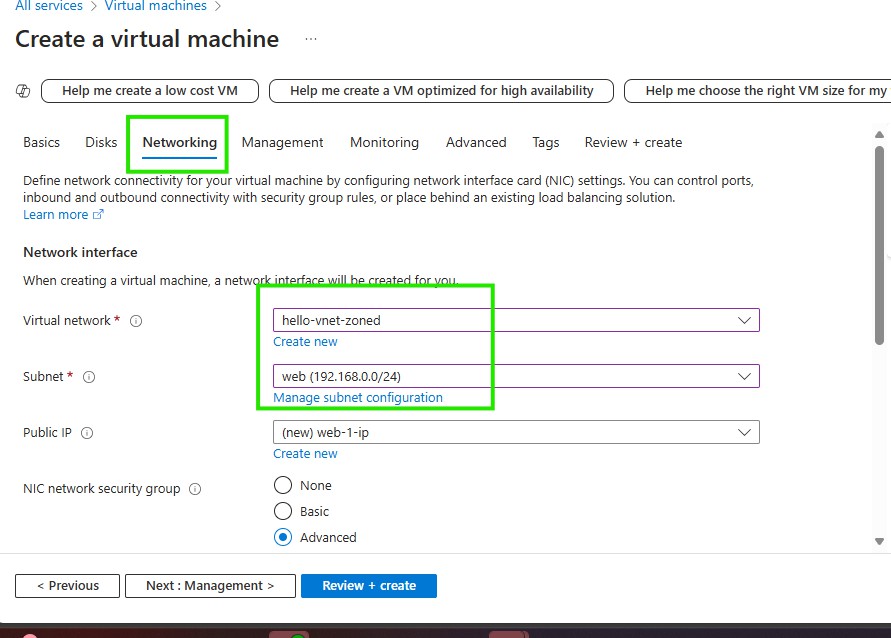
Lets create a Network security group (NSG equivalent to NACL of AWS) Azure uses NSG for both network interface and subnet

[Refer Here](https://learn.microsoft.com/en-us/azure/virtual-network/manage-network-security-group?tabs=network-security-group-portal) for quick start of NSG Lets create an NSG which allows

 ping from any where  http from anywhere

ssh from my ip

Now lets create a linux server in the network with nsg attached



Note: When writing NACL/NSG Rule's priority  start from 300 or above

dont use sequence numbers (300,301) leave some numbers between rules (300,320)