NSG – Network Security Group

1. It is a virtual Firewall
2. Used to Filter Network Inbound and outbound Network Traffic
3. It supports any TCP and UDP Protocols (port no 0-65535)
4. It supports for allow and deny rules
5. NSG rules are processed based on the Priority, If the rules are conflicted lowest priority with take higher precedence

Rule Name	Priority	Protocol	Service	Port no	Action
RDP Rule1	100	TCP	RDP	3389	Allow
RDP Rule2	200	TCP	RDP	3389	Deny

6 . NSG rules are associated with Azure VMs and Subnets

7, By default NSG deny all the inbound external traffic

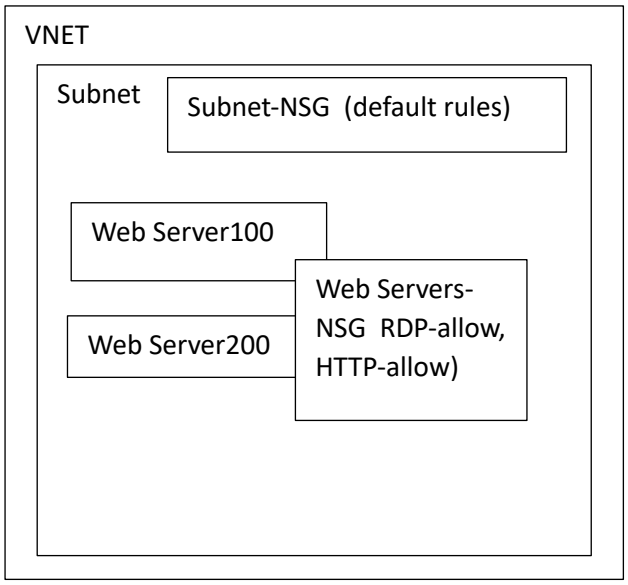
8, By default NSG allow all the outbound external traffic

EX-1 If the NSG is not associated with any Azure VMS and subnets what is the security level?

Security Level: fully blocked

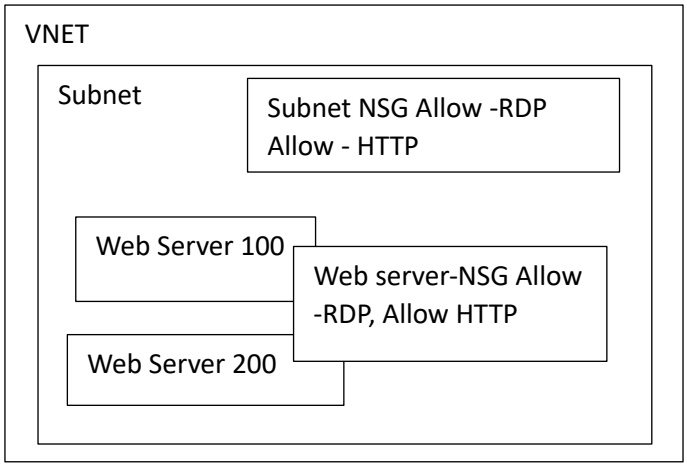
Subnet NSG

Ex-1 In this below example subnet-nsg has default rules and VM NSG has RDP allow and HTTP allow, when you establish request the 65500-default rule will apply and all the connections will be blocked at subnet level



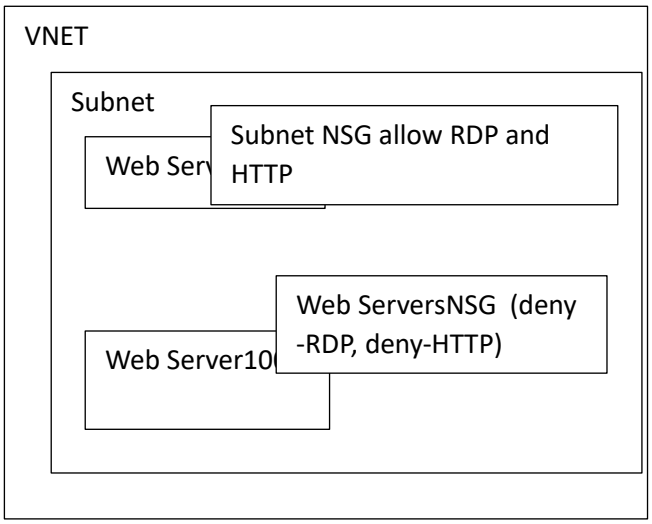
Ex-2

In below Example subnet level and VM Level custom rules are configured for RDP and HTTP as allow so we can connect and succeed

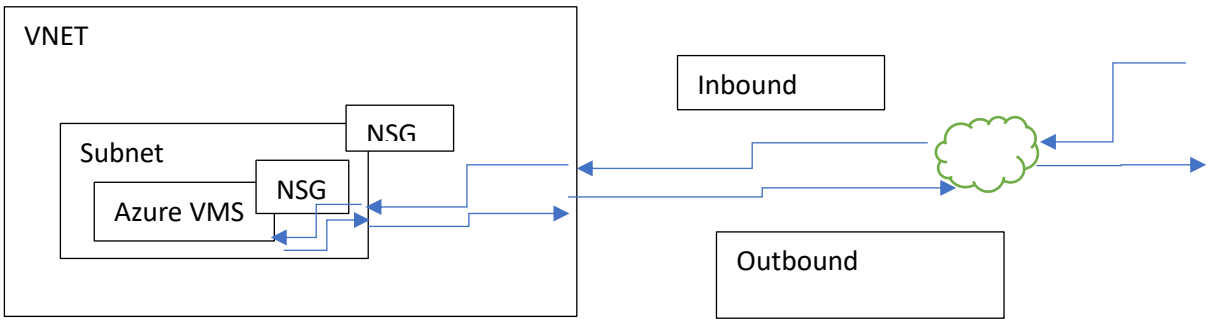


Ex-3

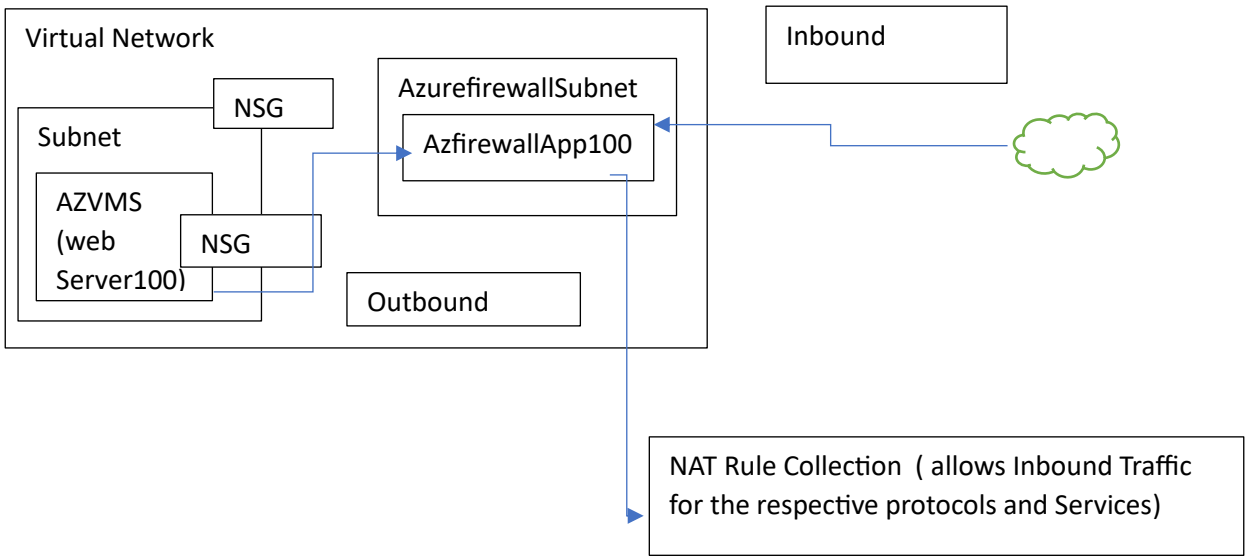
In the Below example Even though RDP and HTTP allowed at subnet level, VM NSG is having deny rules so again RDP and HTTP Connection is blocked



Before Azure Firewall Appliance



After Azure Firewall Appliance Deployment



NAT rule Collection100							
Rule name	Source Type	Source	Protocol	Des Port	Destination	Translated address	Translated Port
RDPRule100	Ipaddress	*	TCP	Firewall RDP PortNo (3389)	Firewall Associated Public Ip address	Private Ip address of Azure VM (web Server	Azure VMS (web Server Portno for RDP - 3389