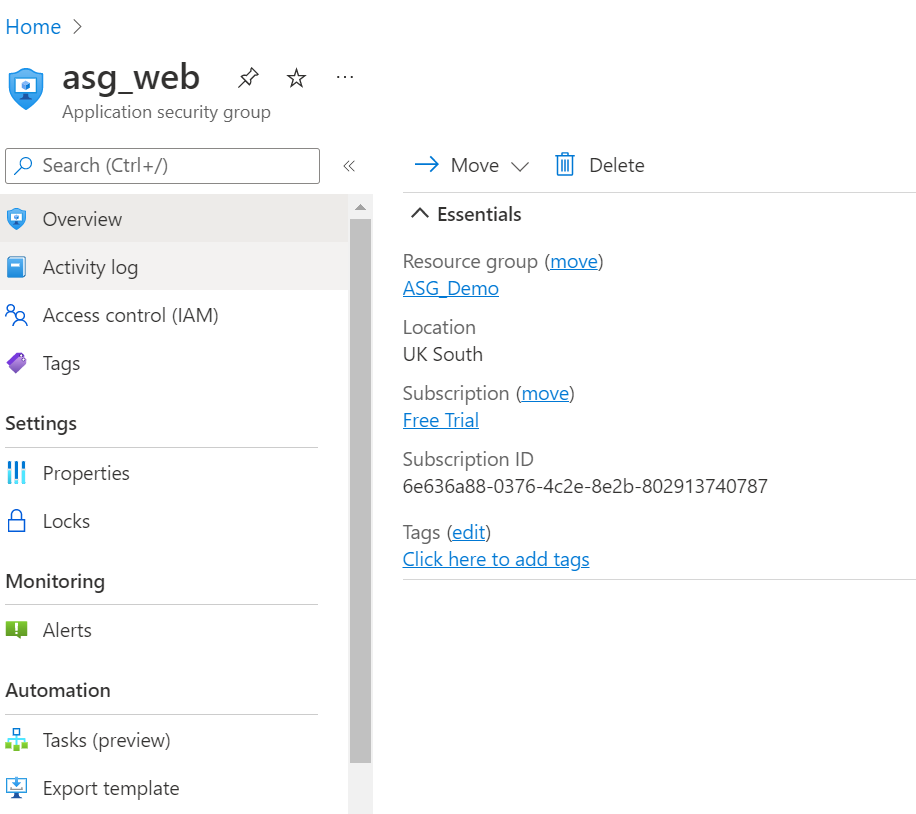
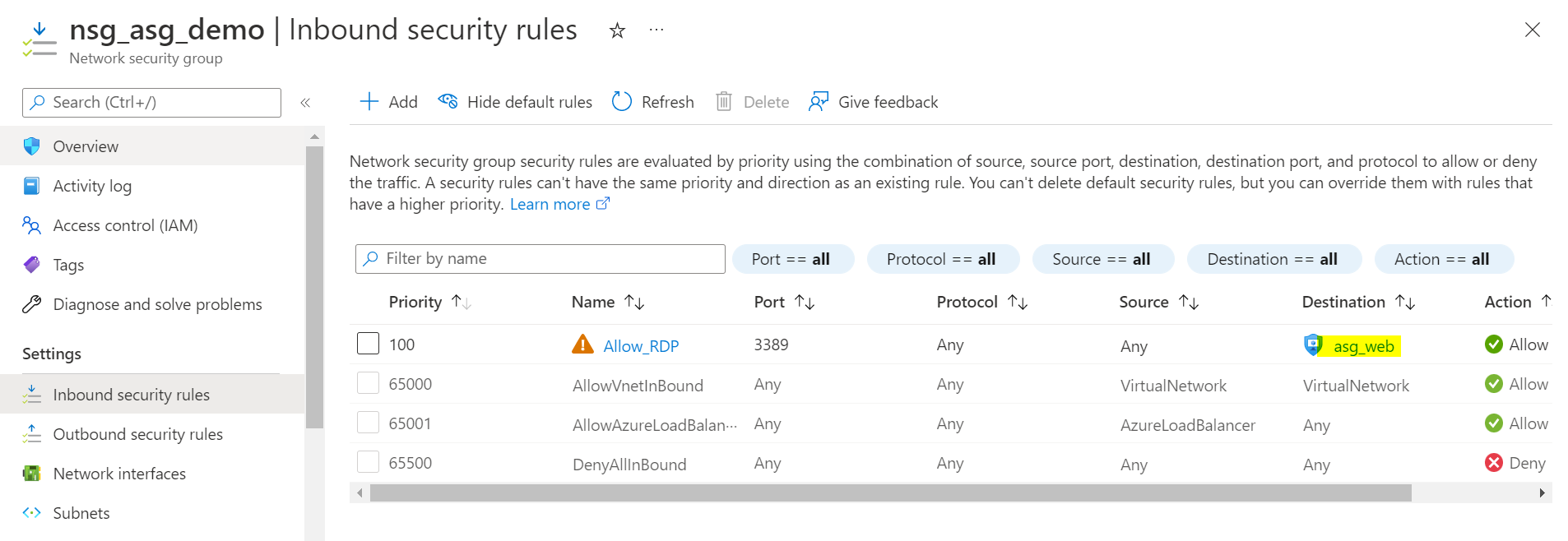
Application Security Group (ASG) - Restrict RDP only to Web– DEMO

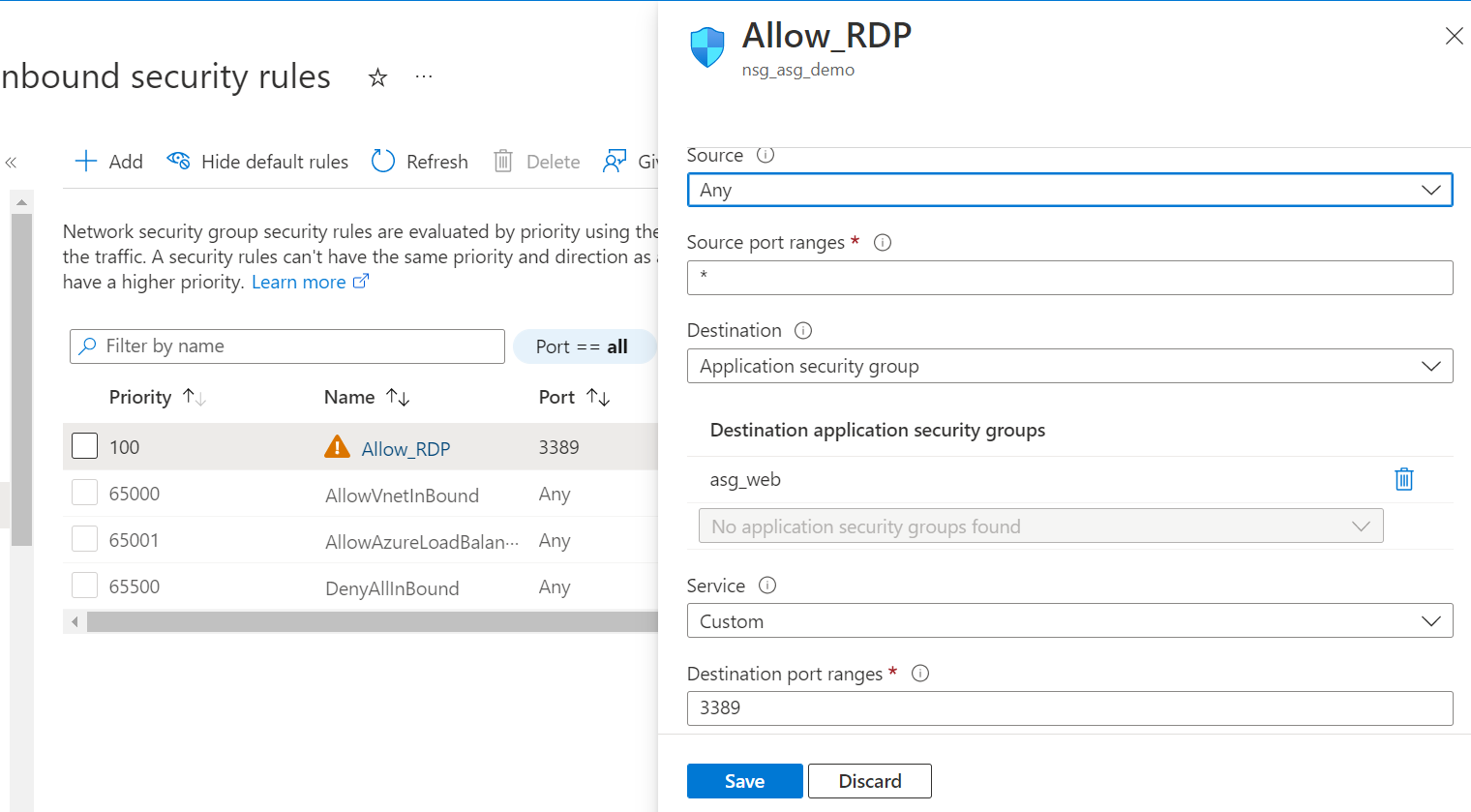
Step-by-Step Configuration

1. Log in to the Azure portal at  [https://portal.azure.com](https://portal.azure.com/).
2. Create an RG “asg\_demo” on any one of the regions say “(Europe) UK South” wherein free VM is available for your (free?) subscription.
3. Create a vnet1 with address range 10.0.0.0/23
4. Split in to 2 subnets.
   * Subnet1 10.0.0.0/24
   * Subnet 10.0.1.0/24
5. Create Application Security Group (ASG) “asg\_web”. There is no config to be done here since it’s just a container on which you will group the VMs and attach with security rules from NSG

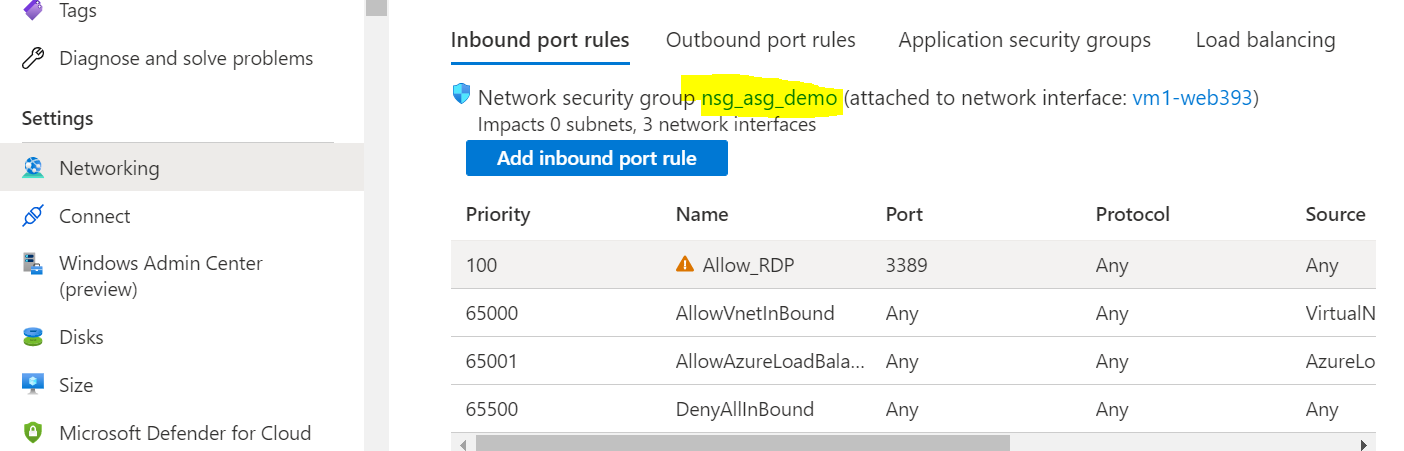


1. Create a NSG “nsg\_asg\_demo” with below rules.

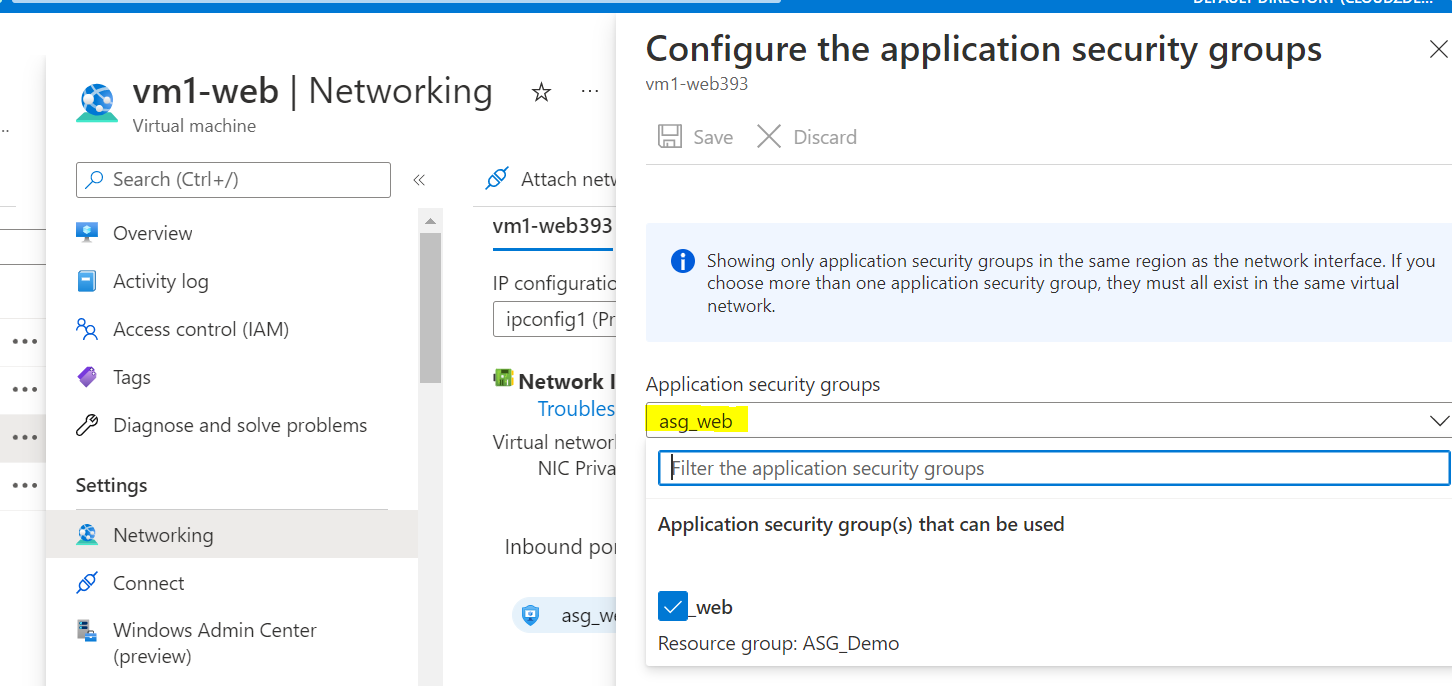


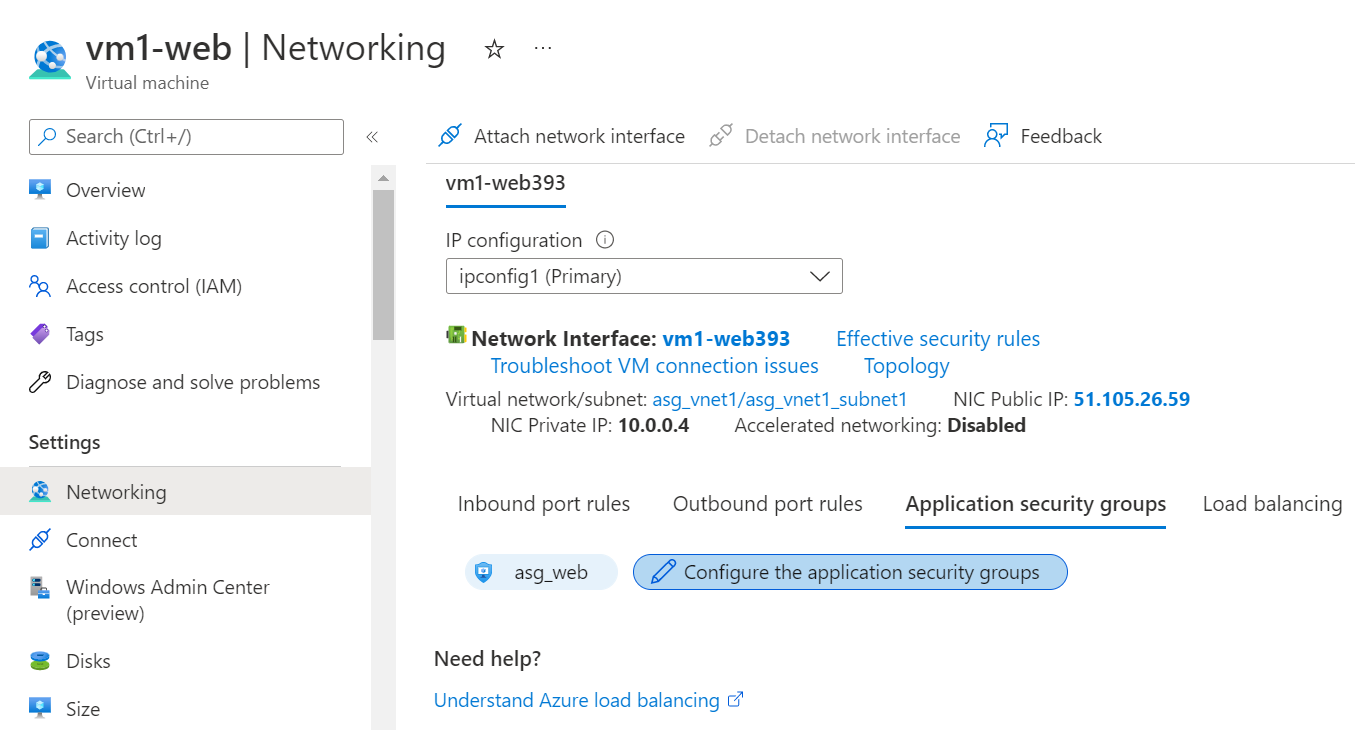


1. Create a VM for web such as “VM1-web” on subnet1 and say its NIC address going to be 10.0.0.4
   * While creating VM, in “Networking” section, choose advance option, and select “nsg\_asg\_demo” as NSG instead letting you azure to create a new one on its own which is default option.



* + Once VM is created, configure its “Networking” by selecting “asg\_web” as its ASG.





1. Create a VM for web such as “VM2-web” on subnet2 and say its NIC address going to be 10.0.1.4
   * Follow all same steps of “VM1-web”
2. Create a VM for DB such as “VM1-DB” on subnet1 and say its NIC address going to be 10.0.0.5
   * Follow all same steps of “VM1-web” but except configuring its “Networking” by selecting “asg\_web” as its ASG.
   * So the point is that we put or isolate only web VMs in to a ASG and apply NSG rule only for those.
3. Now RDP web VMs and ensure you’re able to and you should not be able to RDP to DB VM1-DB