NSG

A network security group (NSG) in Azure is the way to activate a rule or access control list (ACL), which will allow or deny network traffic to your virtual machine instances in a virtual network. NSGs can be associated with subnets or individual virtual machine instances within that subnet. When an NSG is associated with a subnet, the ACL rules apply to all Virtual Machine instances of that subnet. In addition, you can further restrict traffic to an individual virtual machine by associating an NSG directly to that virtual machine.

Considerations around configuring Network Security Groups

Default rules

All network security groups contain a set of default rules. You cannot delete the default rules, but since they are assigned the lowest priority, they can be replaced by the rules you create.

As shown in the following predetermined rules, traffic that originates and terminates in a virtual network is allowed in both the inbound and outbound directions. Although Internet connectivity is allowed for the exit address, it is blocked for the entry address by default. There is a default rule to allow the Azure load balancer to poll the status of virtual machines and role instances. You can override this rule if you are not going to use a load balanced set.

Association of network security groups

You can associate a network security group with virtual machines, NICs, and subnets, depending on the deployment model you use:

* **Association of a network security group to a virtual machine (only classical implementations)**: When you associate a network security group with a VM, the network access rules of the network security group apply to all traffic that enters and leaves the VM.
* **Association of a network security group to a NIC (only implementations of the Resource Manager)**: By associating a network security group with a NIC, the network access rules of the network security group apply only to that NIC. This means that in a virtual machine with several NICs, the fact that a network security group applies to a single NIC does not affect the traffic linked to other NICs.
* **Association of a network security group to a subnet (all implementations)**: When associating a network security group with a subnet, the network access rules of the network security group are applied to all the IaaS and PaaS resources of the subnet.

You can associate different network security groups to a virtual machine (or NIC, depending on the deployment model) and to the subnet to which a NIC or virtual machine is linked. When this happens, all network access rules are applied to traffic, by priority in each network security group, in the following order:

Inbound traffic:

1. Network security group applied to subnet: If a network security group on the subnet has a matching rule to deny traffic, the packet will be discarded.
2. Network security group applied to NIC (Resource Manager) or VM (classic): If the network security group of the virtual machine or the NIC has a matching rule to deny traffic, the packet will be discarded in the virtual machine or the NIC, even if the network security group on the subnet has a match rule to allow traffic.

Outbound traffic:

1. **Network security group applied to a NIC (Resource Manager) or VM (classic)**: If the network security group of the virtual machine or the NIC has a matching rule to deny traffic, the packet will be discarded.
2. **Network Security Group applied to the subnet**: If the network security group on the subnet has a matching rule to deny traffic, the packet will be discarded here, even if the network security group of the virtual machine or the NIC has a matching rule to allow traffic.

Virtual network and subnet design

Because network security groups can be applied to subnets, you can minimize the number of them by grouping resources by subnet and applying these groups to subnets. If you decide to apply network security groups to subnets, you may find that existing virtual networks and existing subnets have been defined without considering them.

Therefore, you may need to define new subnets and virtual networks to fit the design of network security groups. In addition, you must implement new resources in the new subnets. Then, you could define a migration strategy to move the existing resources to the new subnets.

Special rules

You must also take into account the special rules listed below. Make sure that it does not block the traffic allowed by those rules because, otherwise, the infrastructure will not be able to communicate with essential Azure services.

* **Virtual IP of the host node**: Basic infrastructure services, such as DHCP, DNS and status tracking, are provided through the IP address 168.63.129.16 of the virtualized host. This public IP address belongs to Microsoft and will be the only virtualized IP address that will be used in all regions for this purpose. This IP address is assigned to the physical IP address of the server machine (host node) that hosts the virtual machine. The host node acts as a DHCP relay, DNS recursive resolution, probe source, load balancer maintenance probe, and equipment maintenance probe. Communication with this IP address should not be considered as an attack.
* **Licenses (key management service)**: Windows images running on virtual machines must be licensed. To do this, a license request must be sent to the host servers of the key management service that administer those queries. This will always be done at the 1688 exit port.

ICMP Traffic

The rules of the current network security groups only allow TCP or UDP protocols. There is no specific ICMP tag. However, ICMP traffic is allowed within a virtual network by default thanks to the virtual network rules of entry (default 65000 input rule) that allow traffic to and from any port and protocol within the virtual network.

Subnets

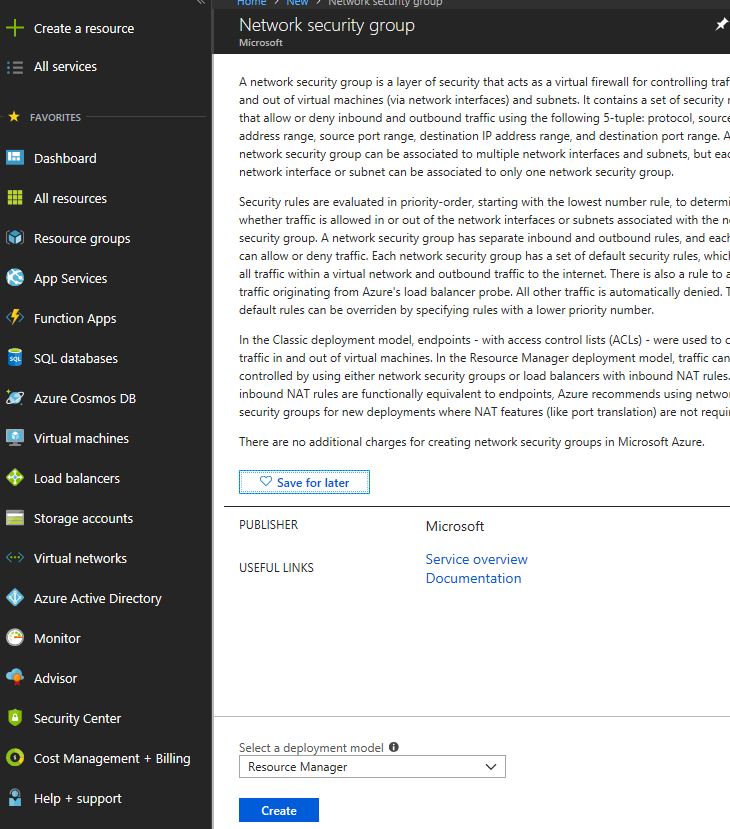
* Consider the number of levels required by the workload. Each level can be isolated by using a subnet, and a network security group is applied to each subnet.
* If you need to implement a subnet for a VPN gateway or an ExpressRoute circuit, be sure NOT to apply a network security group to that subnet. If it does, connectivity between local environments or between virtual networks will not work.
* If you need to implement a virtual appliance, be sure to do it on your own subnet, so that your user-defined routes (UDR) can work correctly. You can implement a subnet level network security group to filter traffic in and out of this subnet.

Load balancers

* Consider the NAT and load balancing rules for each load balancer used by each of the workloads. These rules are linked to a back-end group that contains NICs (implementations of the Resource Manager) or virtual machines and role instances (classic implementations). Consider creating a network security group for each back-end group, so that only assigned traffic is allowed through the rules implemented in the load balancers. This way, it is guaranteed that the traffic that arrives directly to the back-end group, without going through load balancing, is also filtered.
* In classic deployments, create connection points that assign ports of a load balancer to ports of virtual machines or role instances. You can also create your own load balancer with individual public access in an implementation of the Resource Manager. If you are restricting traffic to the virtual machines and role instances that are part of a back-end group of a load balancer by using network security groups, note that the destination port for the traffic Incoming is the real port of the virtual machine or role instance, and not the port that exposes the load balancer. Also note that the address and the source port for the connection to the virtual machine is the port and the address on the remote computer on the Internet.
* Similar to publicly accessible load balancers, when you create network security groups to filter traffic from an internal load balancer (ILB), you must understand that the source port and the applied address range are those of the equipment that originates the call, and not those of the load balancer. And the port and the range of destination addresses are related to the equipment that receives the traffic, and not the load balancer.

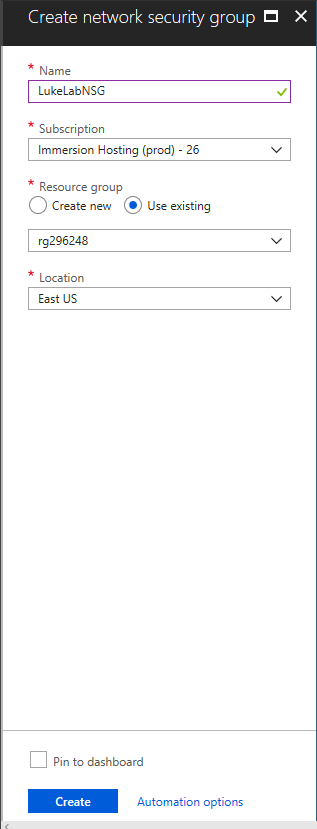
Step by Step configure a security group in Virtual Machine in Azure

We enter our portal and look for our resource group

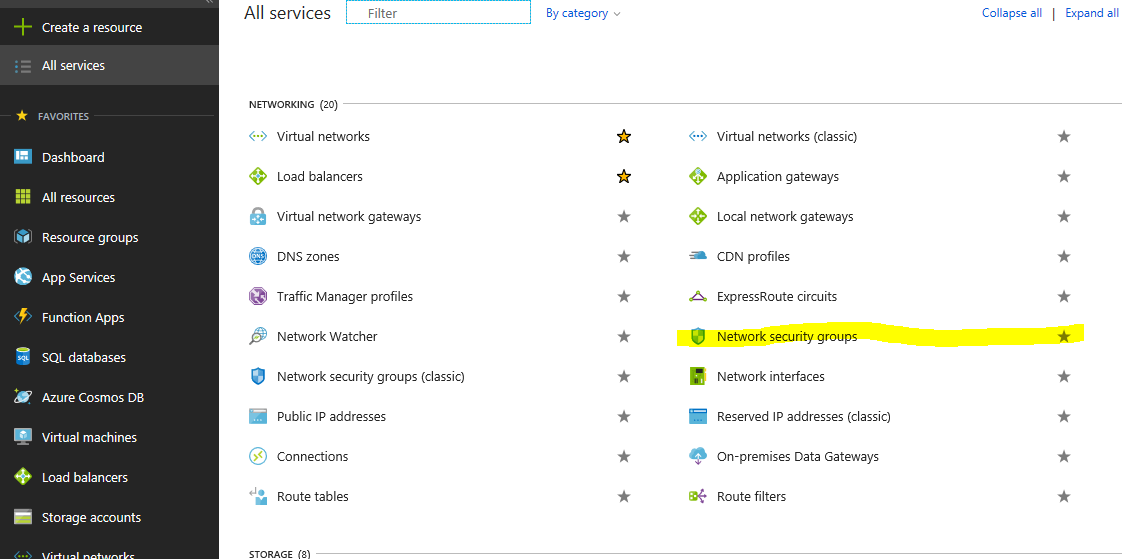


We go to the resource group panel and click on Add

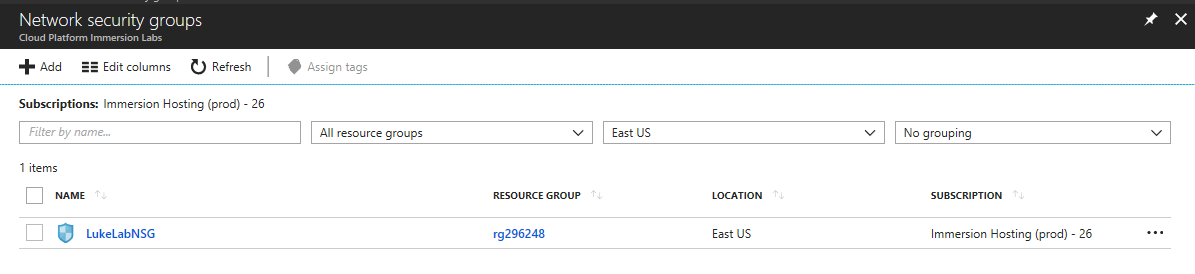
Assign the name of our security group and select our resource group and click on create



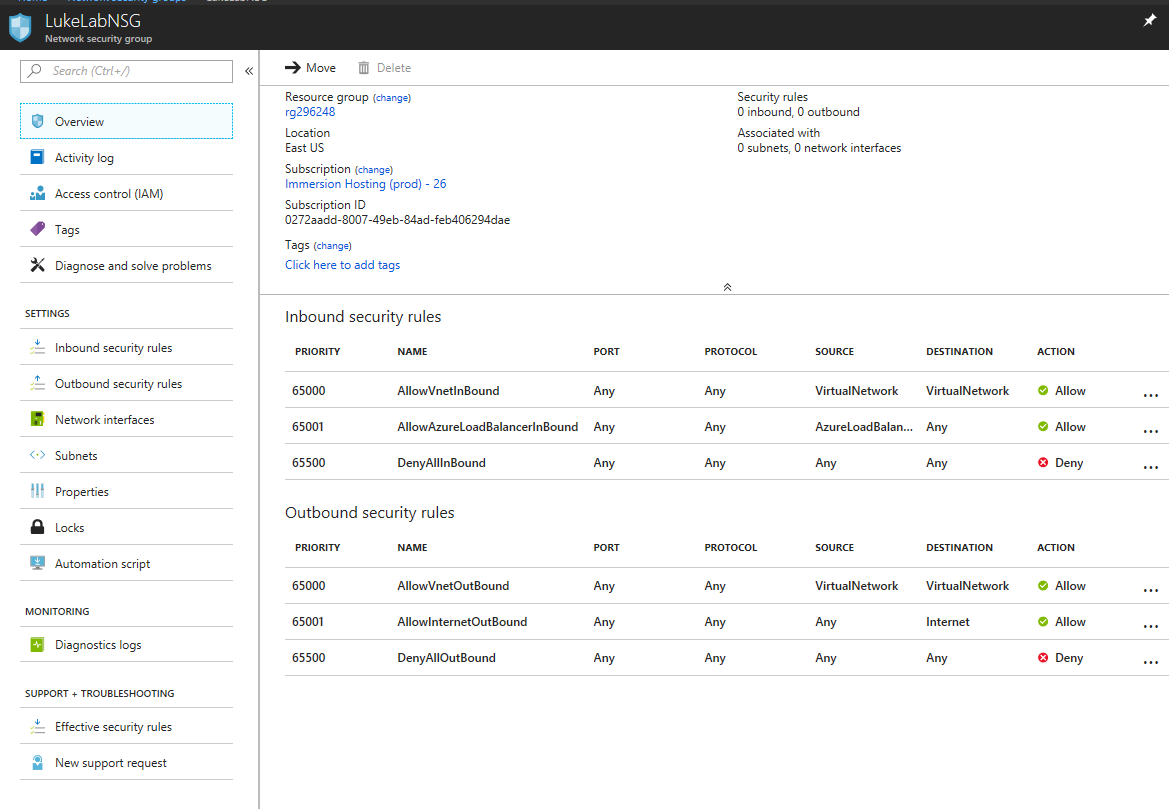
We wait for the NSG to deploy and once completed, we can view it by clicking on All Services on the left-hand side and selecting Network Security Groups:



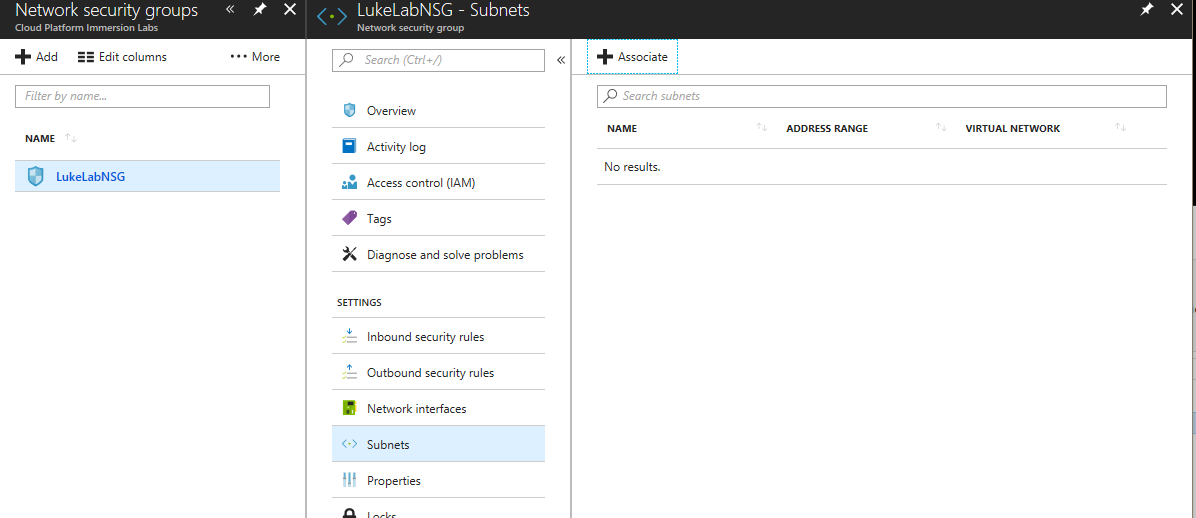
We can now see our new NSG, and we can further configure it by clicking on the name:



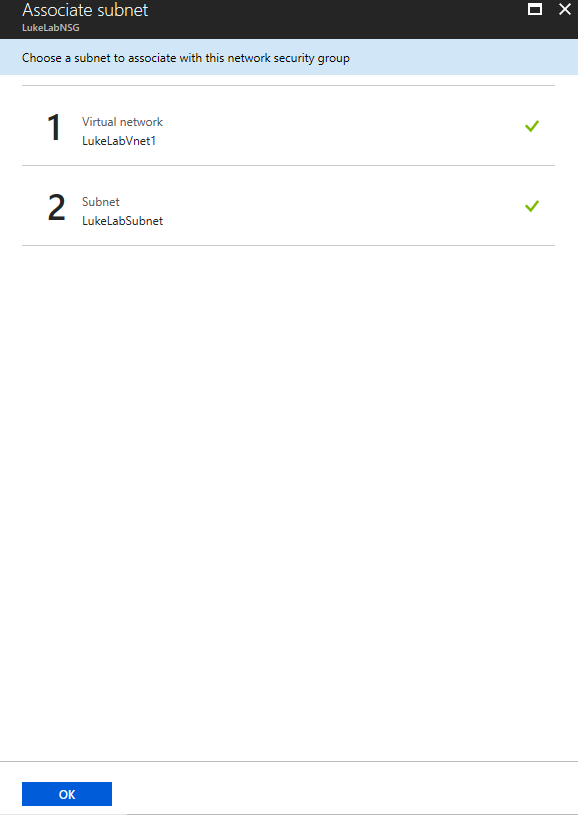
We need to assign a subnet to associate this NSG with, select Subnets on the left-hand side:



Now click the Associate button so we can find our subnet and the virtual network that we created in part 1. Remember, we created this when we set up the Virtual Network:



We can now see that we have the LukeLabVnet1 virtual network that we created and the LukeLabSubnet assigned to this network security group. Click Ok to configure:



Creation of Security Groups in Azure Via PowerShell

#Defining security rules for Virtual Machine entry

$ rule1 = New-AzureRmNetworkSecurityRuleConfig -Name rdp-rule -Description “Allow RDP” -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix Internet -SourcePortRange \* -DestinationAddressPrefix \* -DestinationPortRange 3389

New-AzureRmNetworkSecurityGroup -ResourceGroupName $ ResourceGroupName -Location $ Location -Name “SECURITY” -SecurityRules $ rule1

#Creating Virtual Machine entry security rule

New-AzureRmVM -ResourceGroupName $ ResourceGroupName -Location $ Location -VM $ vm

A Set of prioritised stateful inbound rules

A Set of prioritised stateful outbound rules

Each rule allows or blocks based on

* Source address/location
* Destination address/location
* Source protocol (TCP/UDP)
* Destination protocol (TCP/UDP)
* Source port(range)
* Destination port (range)
* Direction (in/out)
* Priority (they have general/granular rules)

Every NSG contains a set of default stateful inspection rules

HOW TO ADD ADDITIONAL NIC CARDS to YOUR AZURE VM

MAY BE TO SEGGREGATE FRINT END TRAFFIC TO BACKEND TRAFIC

1. Your VMM has to be in stopped or de allocated state
2. Go to your VM, Go to Networking
3. Create
4. Give it a name
5. Select subnet
6. Select Ip Address
7. Select nsg
8. Attach Network Interface