## Network Security Groups and Public IPs

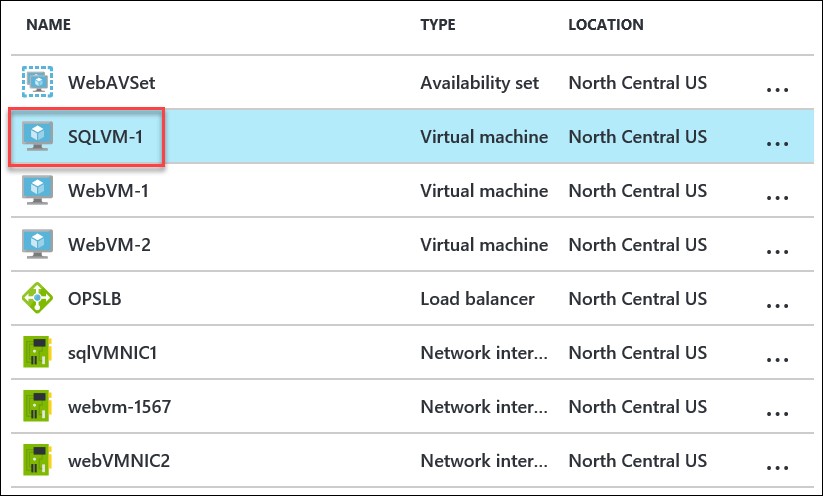
### Lab Overview

In this lab, you will create a new Public IP address to the **SQLVM-1** virtual machine and then learn how to restrict access to the public IP using a network security group.

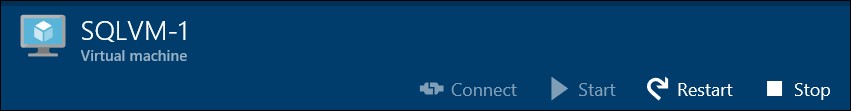
### Exercise 1: Add a Public IP Address

1. Using the Azure Management Portal, click **Browse**, **Resource Groups**, **OpsVMRmRG**.

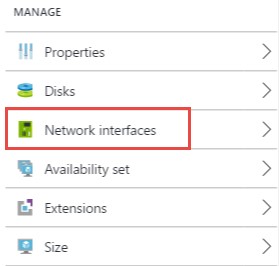
1. In the Summary view click the **SQLVM-1** virtual machine.



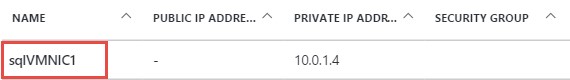
1. Note that the Connect button is disabled on the toolbar. This is because there is no public IP address associated with this virtual machine.



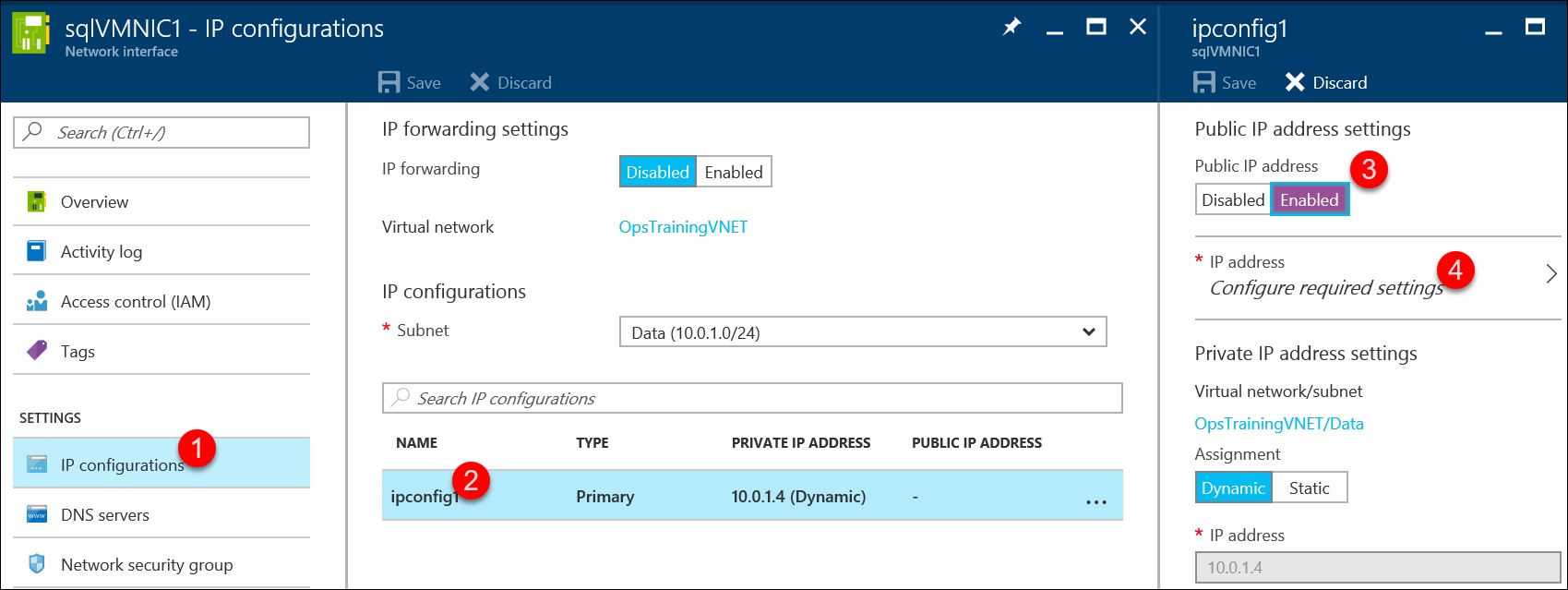
1. To add a public IP, click the **Network interfaces** menu in the **SQLVM-1** settings blade.



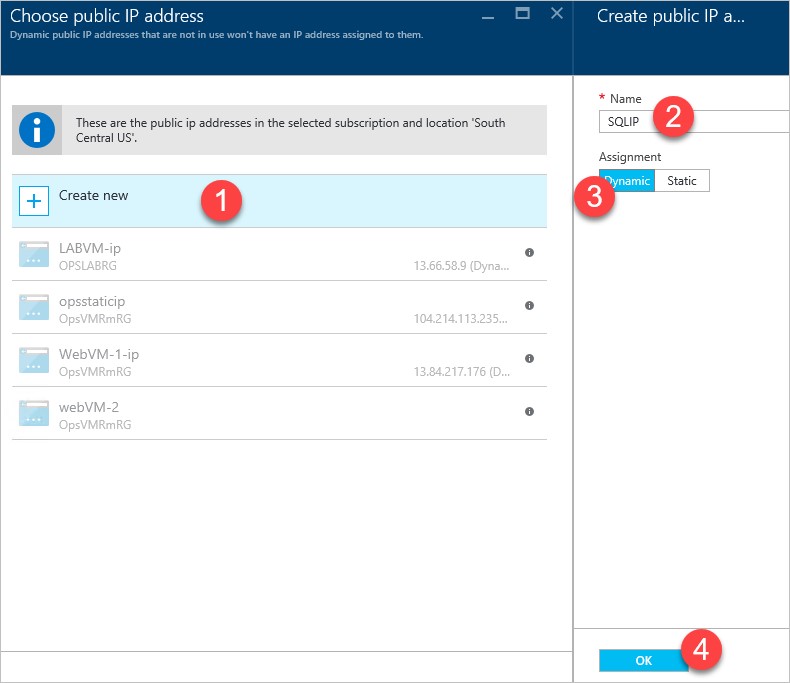
1. Click the **sqlVMNIC1** network interface.



1. Click the **IP configurations** tile on the network interface settings tile. Then click **ipconfig1** under **IP configurations** and click **Enabled.** Finally, click Configure required settings to create a new Public IP address



1. On the Choose public IP address tile, click +Create new, name the IP **SQLIP**, and click **OK**.



1. Click **Save** on the toolbar to save the new IP address and associate it with the network interface.



1. After the update notification shows the changes have completed you can close all the configuration blades for the virtual machine.

10.

Click

**More services**

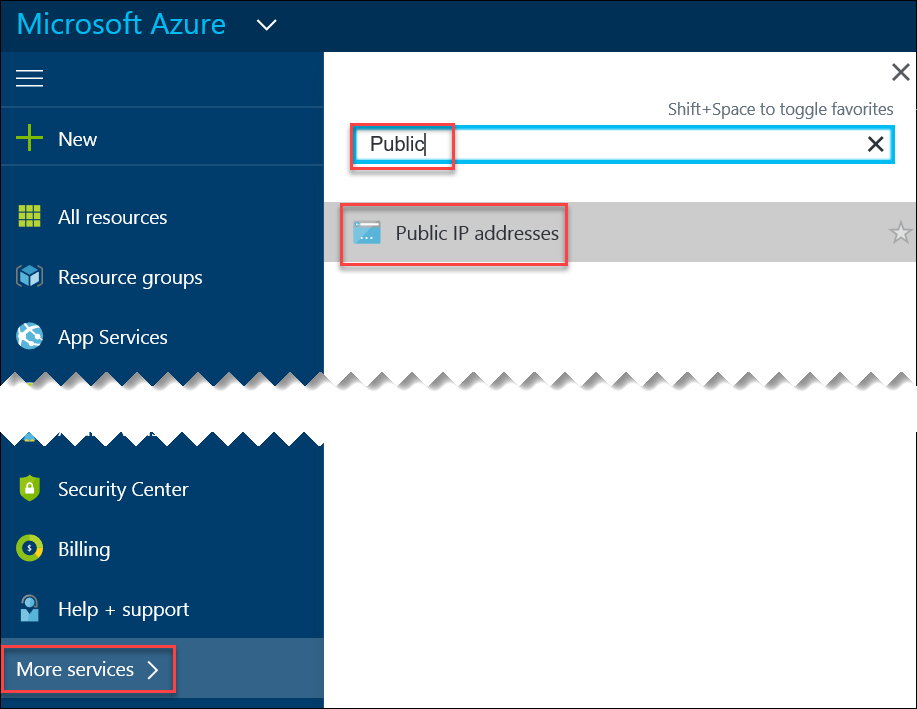
,

**Public IP**

**addresses**

.

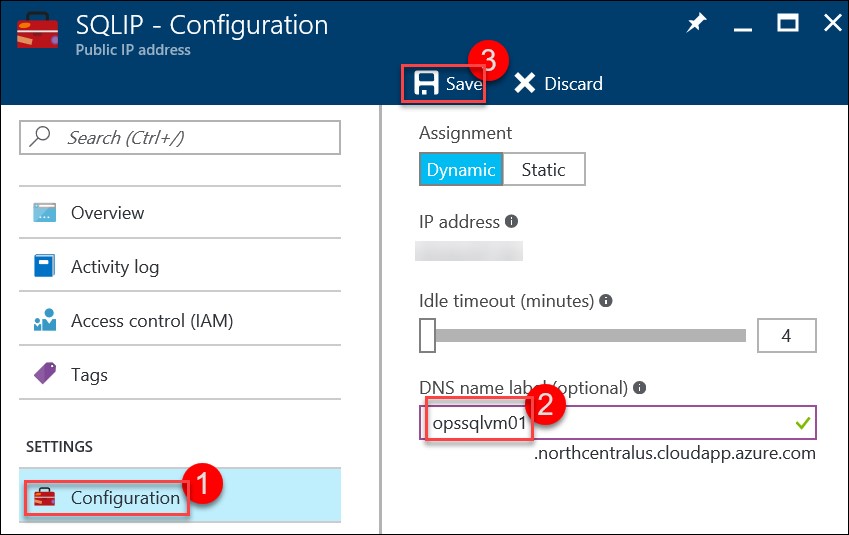




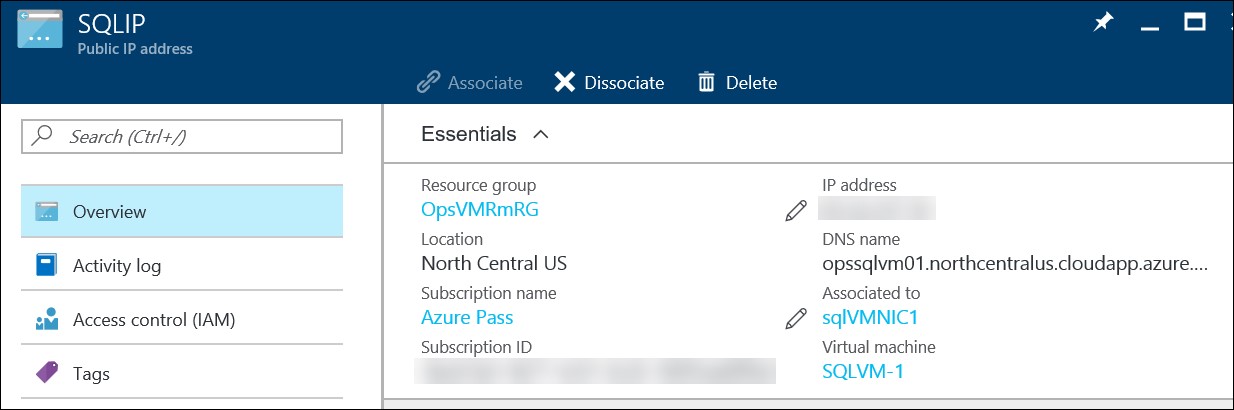
1. Click the **SQLIP** IP address.



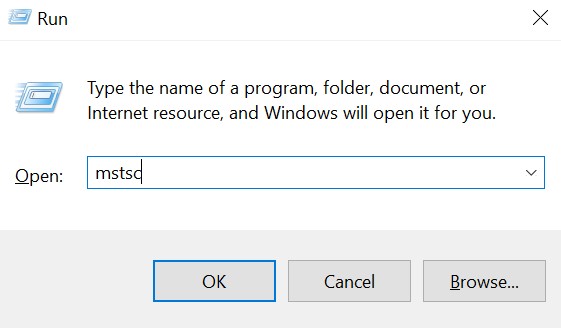
1. On the Settings blade, click **Configuration**, and **specify a unique DNS name label** (ensure the green check mark appears to the right of the text box), and then click **Save**.



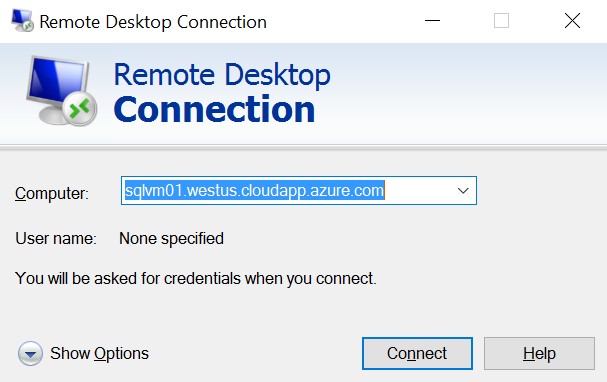
1. After the DNS name is saved copy the full DNS name from the essentials panel of the SQLIP Public IP address.



1. To connect to the virtual machine by launching the remote desktop client manually by typing in **mstsc** in the Windows Run dialog and clicking **OK**.



1. Paste the DNS name into the **Remote Desktop Connection** dialog and click **Connect**.

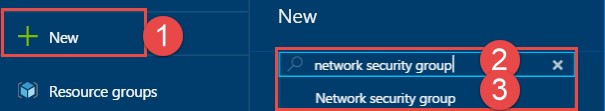


1. Login to the virtual machine using the credentials specified during creation:
   1. Username: **demouser**
   2. Password: **demo@pass123**

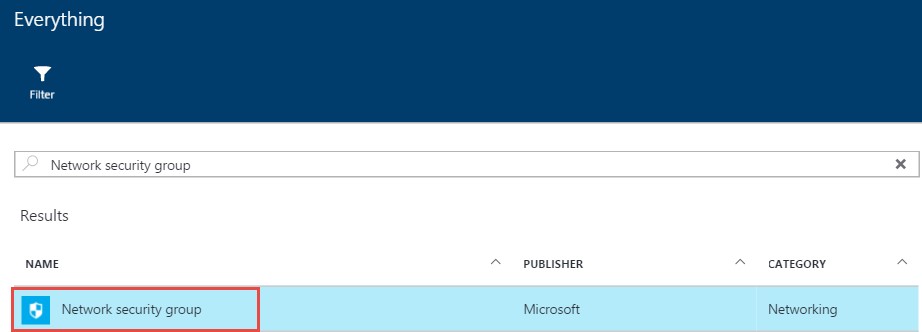
1. After you have verified you can connect, disconnect the session by closing the Remote Desktop Connection client.

### Exercise 2: Create a Network Security Group

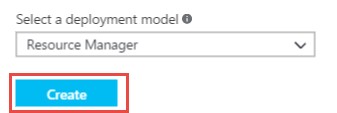
1. Click **New**, and in the Search Marketplace textbox, type in **network security group**, and click the returned **Network security group** result.



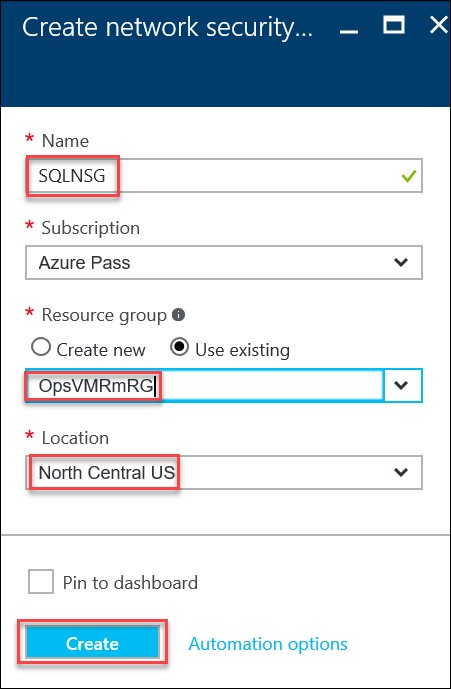
1. Click the returned **Network security group** in the search results.



1. Accept the default of Resource Manager, and click **Create**.

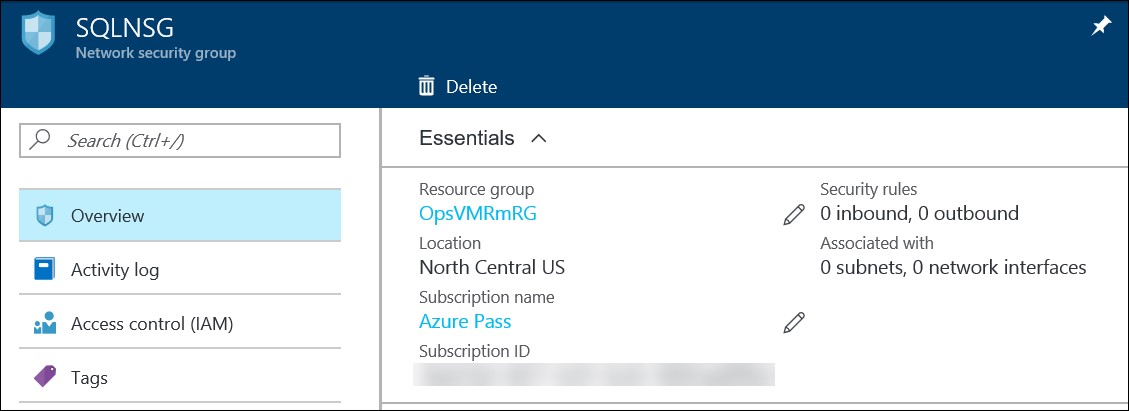


1. Specify the following configuration on the Create network security group dialog:
   1. Name: **SQLNSG**
   2. Resource Group: **select the existing OpsVMRmRG resource group.**
   3. Location: **Choose the same region the virtual machines for the lab are deployed to.**

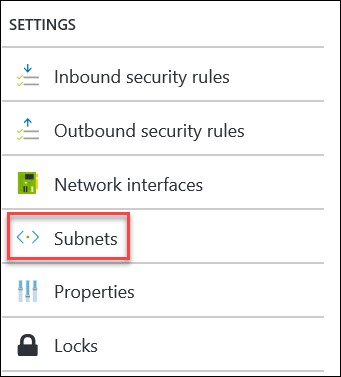


1. Click **Create** after the network security group is configured.

1. Note that the created network security group is not associated with a network interface or subnet yet. This means it is not protecting any resources. Find and open the **SQLNSG** network security group in the **OpsVMRmRG** resource group.



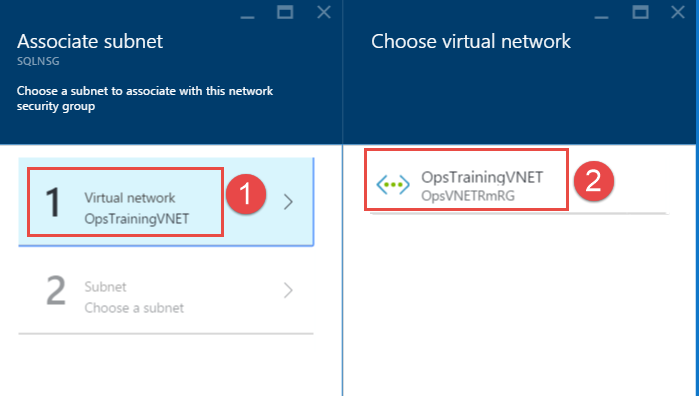
1. On the Settings blade for the Network Security Group, click **Subnets**.



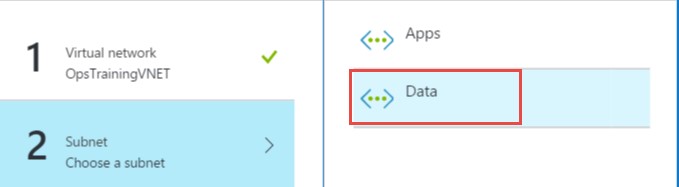
1. Click the **Associate** button on the toolbar.



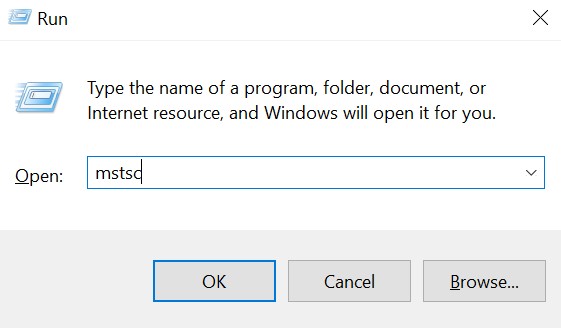
1. Select the **OpsTrainingVNET** in the **OpsVNETRmRG** resource group.



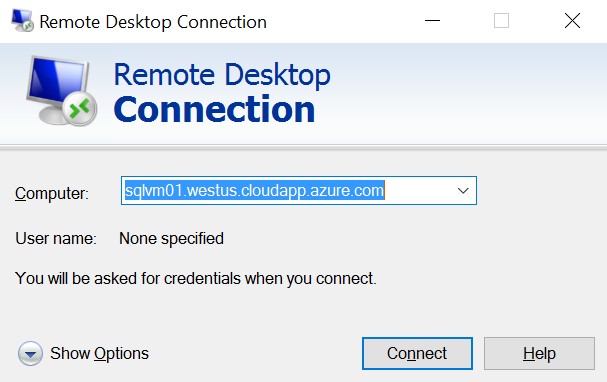
1. Then choose the **Data** subnet, and then click **OK**. After the operation succeeds the network security group rules apply to all traffic in the subnet.



1. Wait 1 – 2 minutes then Launch the remote desktop client again by typing in **mstsc** in the Windows Run dialog and clicking **OK**.



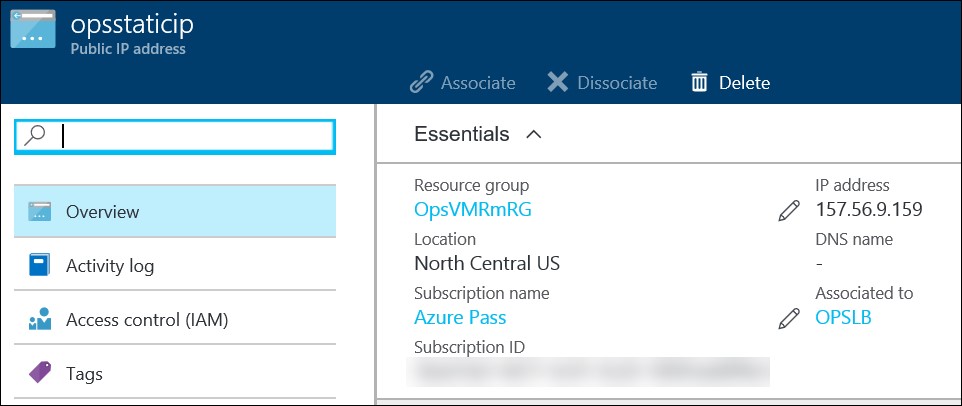
1. Connect to the same DNS name used previously. This time the connection should not succeed because no inbound rule allows it in the network security group.



### Exercise 3: Examine the Network Security Group Default Rules

1. Validate that the web application continues to work by clicking **More Services**, **Public IP Addresses**, and selecting the **opsstaticip** public IP address.

1. Copy the **IP address**, and paste it into a new browser tab instance.

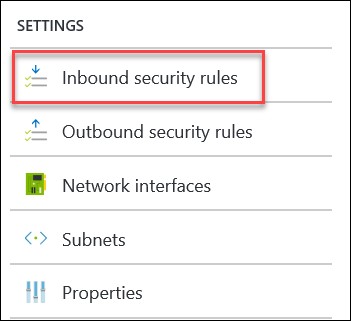


1. The website should still load; this means connectivity to the database still occurs within the virtual network.



1. Open the SQLNSG network security group again, by clicking **More Services**, **Network Security Groups**, and selecting **SQLNSG** using the Azure Management Portal.

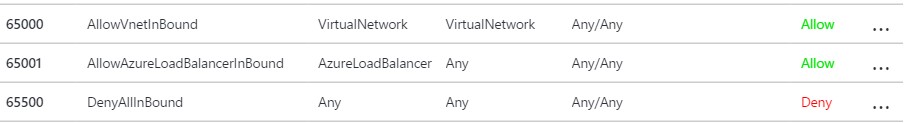
1. On the settings blade click **Inbound security rules**.



1. Click **Default rules** from the toolbar.



1. By default, there are three rules:
   1. **AllowVnetInBound** – allows traffic from any device on the virtual network. This includes any connected virtual networks or local networks from on-premises.
   2. **AllowAzureLoadBalancerInBound** – allows traffic from the load balancer. The SQLVM1 would have to be part of the backend IP configuration of the load balancer to receive traffic, but by default the NSG would allow it.
   3. **DenyAllInBound** – all other traffic is denied.



Tip: Network security group rules are processed based on the priority. Rules are processed based on the lowest priority rule first.

### Lab Summary

In this lab, you created a new Public IP address for the SQLVM-1 virtual machine and then learned how to restrict access to the public IP using a network security group.