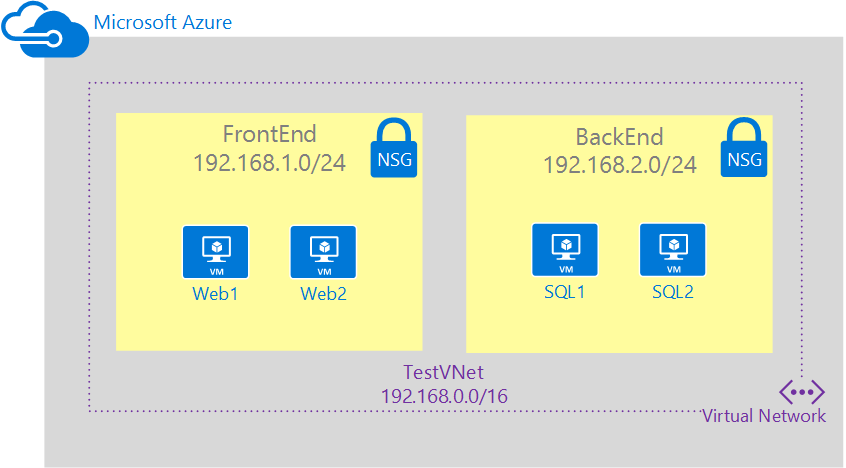
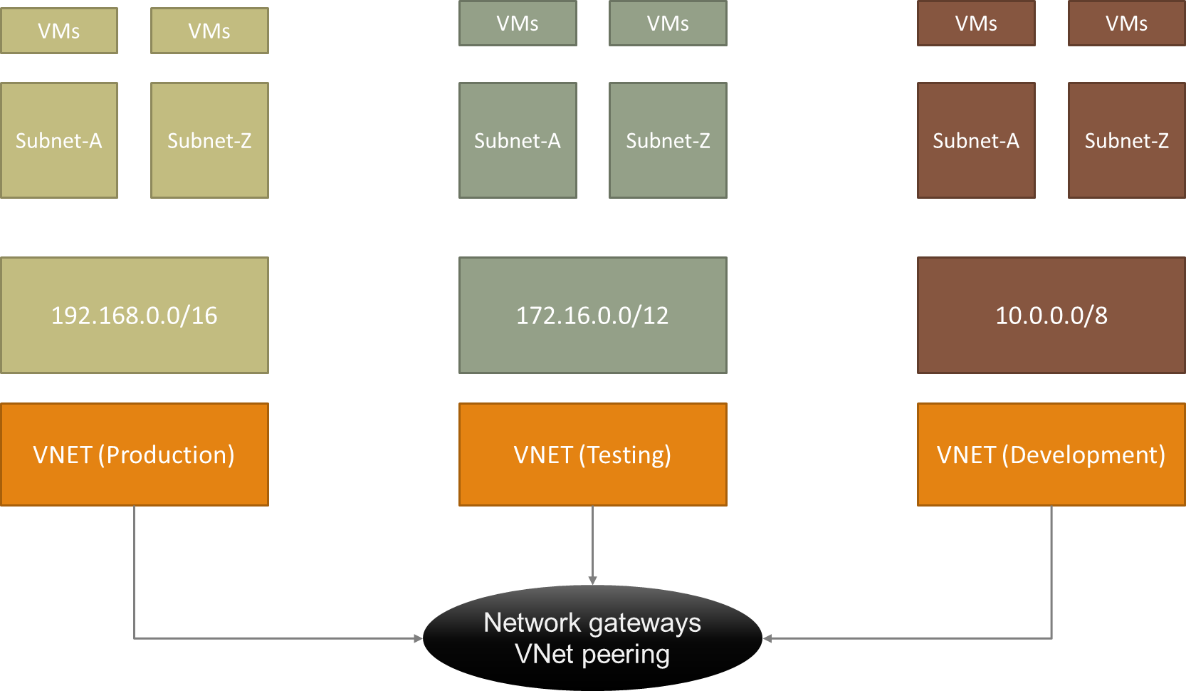
Azure VNet

An **Azure Virtual Network** (**VNet**) is a representation of your own network in the cloud. It is a logical isolation of the **Azure**cloud dedicated to your subscription. ... When you create a **VNet**, your services and VMs within your **VNet** can communicate directly and securely with each other in the cloud



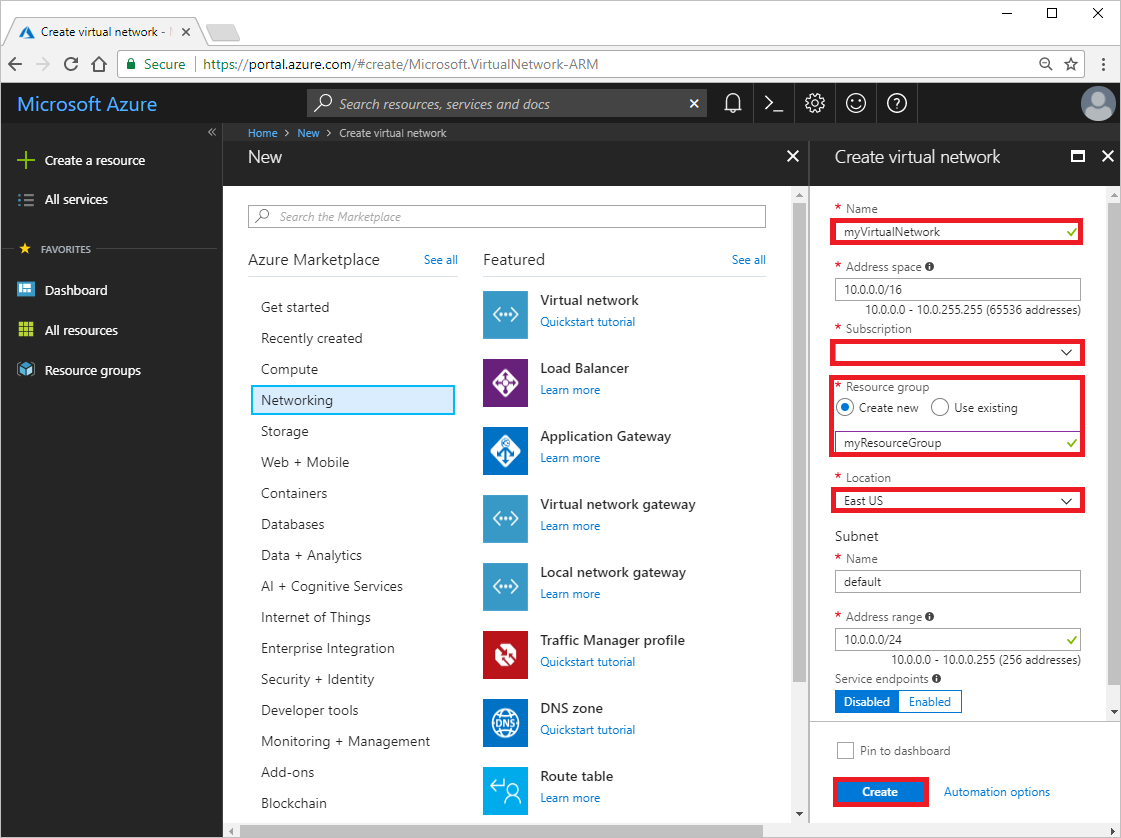


Create a virtual network using the Azure portal

## Create a virtual network

1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. Select **Networking**, and then select **Virtual network**.
3. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **Create**:

| Setting | Value |
| --- | --- |
| Name | myVirtualNetwork |
| Subscription | Select your subscription. |
| Resource group | Select **Create new** and enter myResourceGroup. |
| Location | Select **East US**. |

1. 

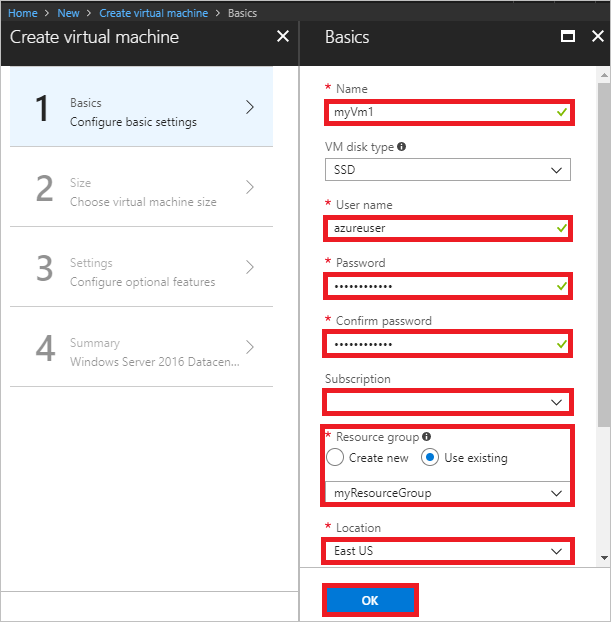
## Create virtual machines

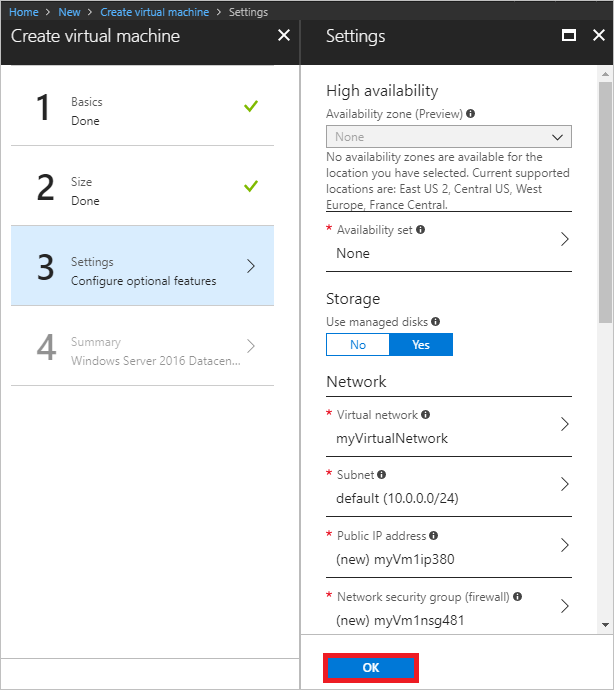
Create two VMs in the virtual network:

### Create the first VM

1. Select **+ Create a resource** found on the upper, left corner of the Azure portal.
2. Select **Compute**, and then select **Windows Server 2016 Datacenter**.
3. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **OK**:

| Setting | Value |
| --- | --- |
| Name | myVm1 |
| User name | Enter a user name of your choosing. |
| Password | Enter a password of your choosing. The password must be at least 12 characters long and meet the defined complexity requirements. |
| Subscription | Select your subscription. |
| Resource group | Select **Use existing** and select **myResourceGroup**. |
| Location | Select **East US** |

1. 
2. Select a size for the VM and then select **Select**.
3. Under **Settings**, accept all the defaults and then select **OK**.



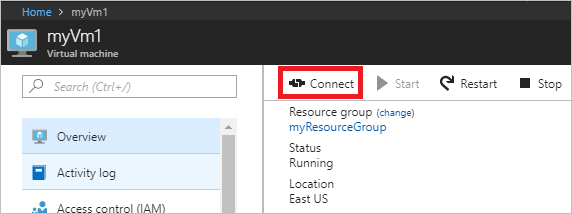
1. Under **Create** of the **Summary**, select **Create** to start VM deployment. The VM takes a few minutes to deploy.

### Create the second VM

Complete steps 1-6 again, but in step 3, name the VM myVm2.

## Connect to a VM from the internet

1. After myVm1 is created, connect to it. At the top of the Azure portal, enter myVm1. When **myVm1**appears in the search results, select it. Select the **Connect** button.



1. After selecting the **Connect** button, a Remote Desktop Protocol (.rdp) file is created and downloaded to your computer.
2. Open the downloaded rdp file. If prompted, select **Connect**. Enter the user name and password you specified when creating the VM. You may need to select **More choices**, then **Use a different account**, to specify the credentials you entered when you created the VM.
3. Select **OK**.
4. You may receive a certificate warning during the sign-in process. If you receive the warning, select **Yes** or **Continue**, to proceed with the connection.

## Communicate privately between VMs

1. From PowerShell, enter ping myvm2. Ping fails, because ping uses the internet control message protocol (ICMP), and ICMP is not allowed through the Windows firewall, by default.
2. To allow myVm2 to ping myVm1 in a later step, enter the following command from PowerShell, which allows ICMP inbound through the Windows firewall:

PowerShellCopy

New-NetFirewallRule –DisplayName “Allow ICMPv4-In” –Protocol ICMPv4

1. Close the remote desktop connection to myVm1.
2. Complete the steps in Connect to a VM from the internet again, but connect to myVm2. From a command prompt, enter ping myvm1.

You receive replies from myVm1, because you allowed ICMP through the Windows firewall on the myVm1 VM in a previous step.

1. Close the remote desktop connection to myVm2.

## Clean up resources

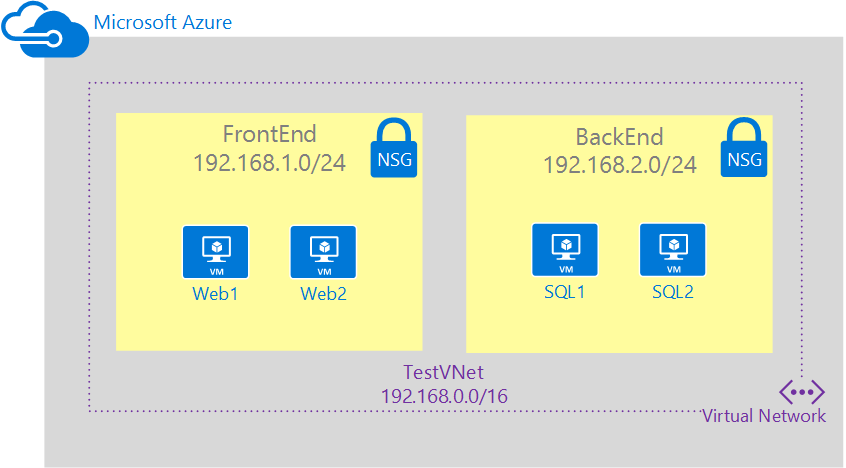
When no longer needed, delete the resource group and all of the resources it contains:

1. Enter myResourceGroup in the **Search** box at the top of the portal. When you see **myResourceGroup** in the search results, select it.
2. Select **Delete resource group**.
3. Enter myResourceGroup for **TYPE THE RESOURCE GROUP NAME:** and select **Delete**.

# Create network security groups using the Azure portal

## Scenario

To better illustrate how to create NSGs, this document will use the scenario below.



In this scenario you will create an NSG for each subnet in the **TestVNet** virtual network, as described below:

* **NSG-FrontEnd**. The front end NSG will be applied to the FrontEnd subnet, and contain two rules:
  + **rdp-rule**. This rule will allow RDP traffic to the FrontEnd subnet.
  + **web-rule**. This rule will allow HTTP traffic to the FrontEnd subnet.
* **NSG-BackEnd**. The back end NSG will be applied to the BackEnd subnet, and contain two rules:
  + **sql-rule**. This rule allows SQL traffic only from the FrontEnd subnet.
  + **web-rule**. This rule denies all internet bound traffic from the BackEnd subnet.

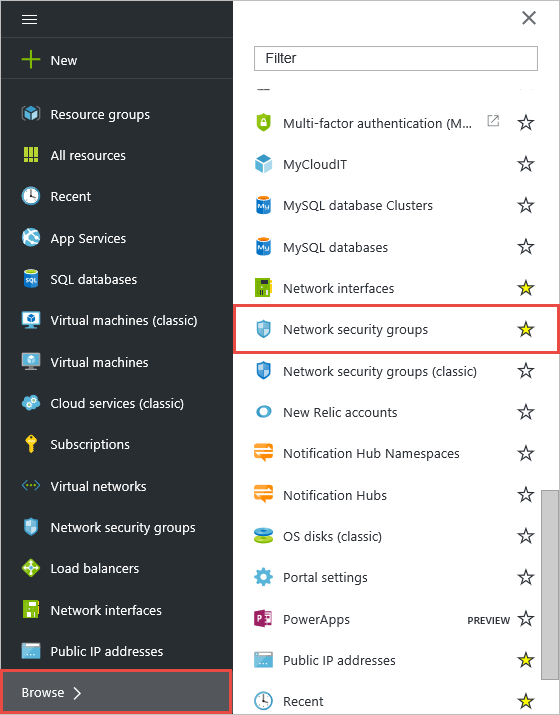
The combination of these rules create a DMZ-like scenario, where the back end subnet can only receive incoming traffic for SQL from the front end subnet, and has no access to the Internet, while the front end subnet can communicate with the Internet, and receive incoming HTTP requests only.

The sample PowerShell commands below expect a simple environment already created based on the scenario above. If you want to run the commands as they are displayed in this document, first build the test environment by deploying this template, click **Deploy to Azure**, replace the default parameter values if necessary, and follow the instructions in the portal. The steps below use **RG-NSG** as the name of the resource group the template was deployed to.

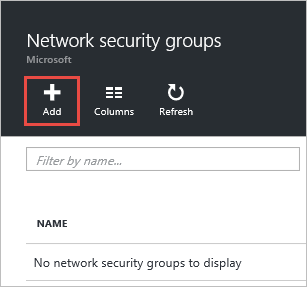
## Create the NSG-FrontEnd NSG

To create the **NSG-FrontEnd** NSG as shown in the scenario above, follow the steps below.

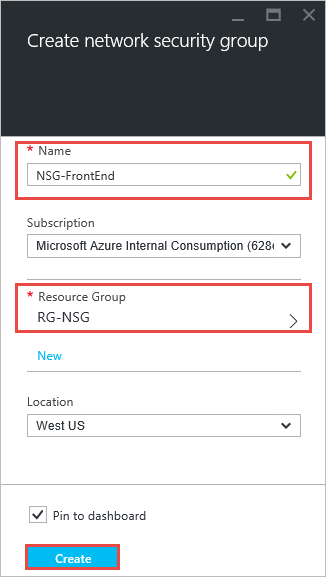
1. From a browser, navigate to http://portal.azure.com and, if necessary, sign in with your Azure account.
2. Click **Browse >** > **Network Security Groups**.



1. In the **Network security groups** blade, click **Add**.



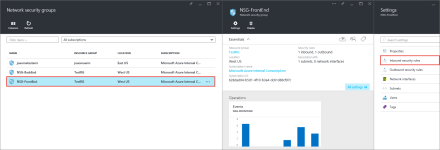
1. In the **Create network security group** blade, create an NSG named NSG-FrontEnd in the RG-NSGresource group, and then click **Create**.



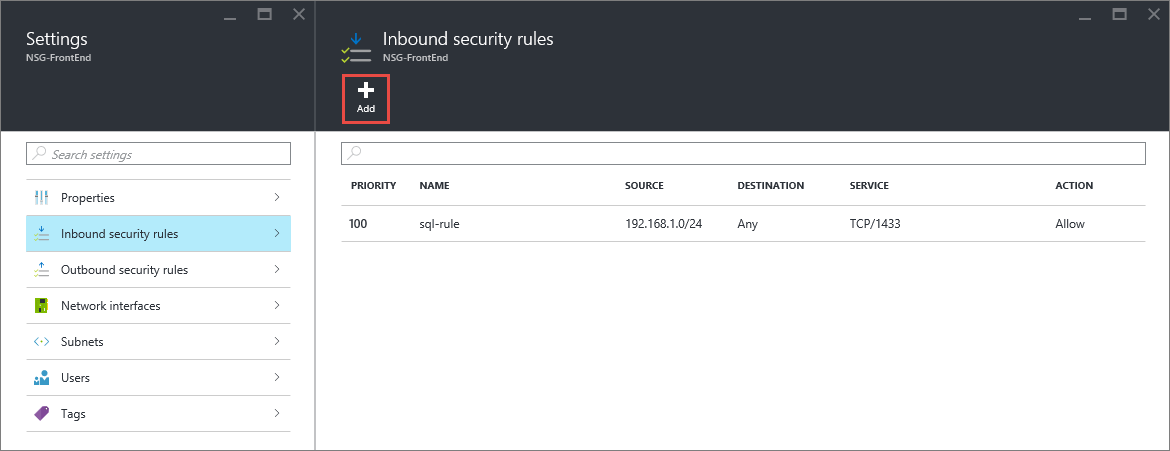
## Create rules in an existing NSG

To create rules in an existing NSG from the Azure portal, follow the steps below.

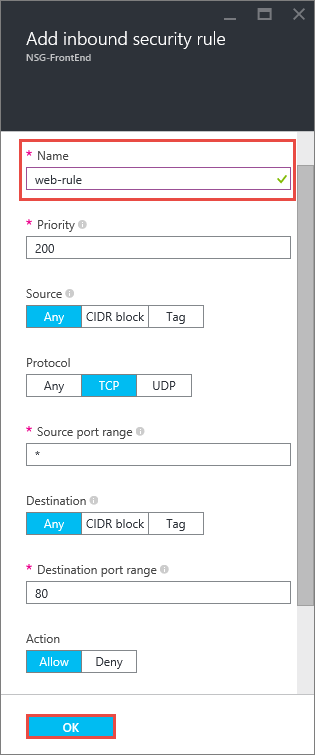
1. Click **Browse >** > **Network security groups**.
2. In the list of NSGs, click **NSG-FrontEnd** > **Inbound security rules**



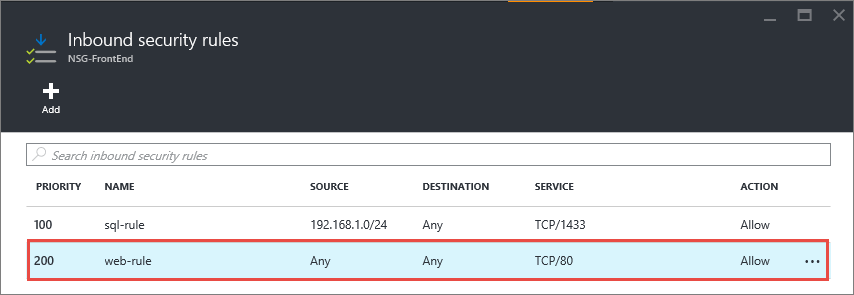
1. In the list of **Inbound security rules**, click **Add**.



1. In the **Add inbound security rule** blade, create a rule named web-rule with priority of 200 allowing access via TCP to port 80 to any VM from any source, and then click **OK**. Notice that most of these settings are default values already.



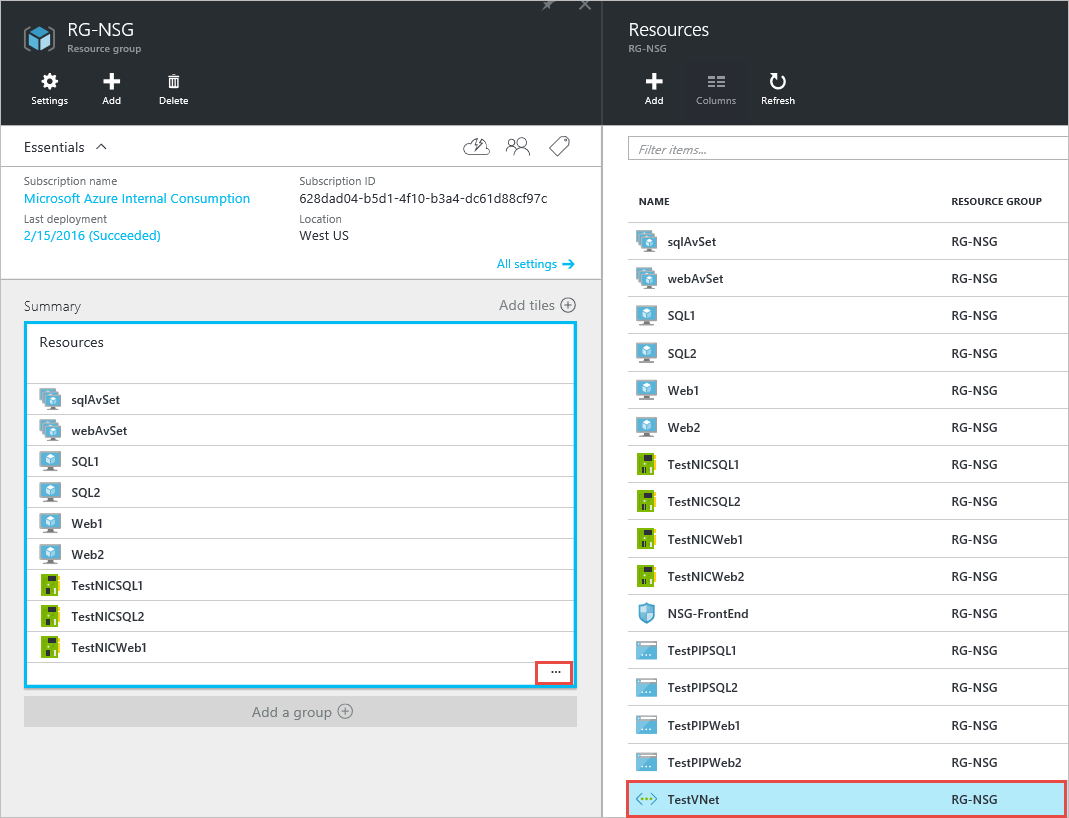
1. After a few seconds you will see the new rule in the NSG.



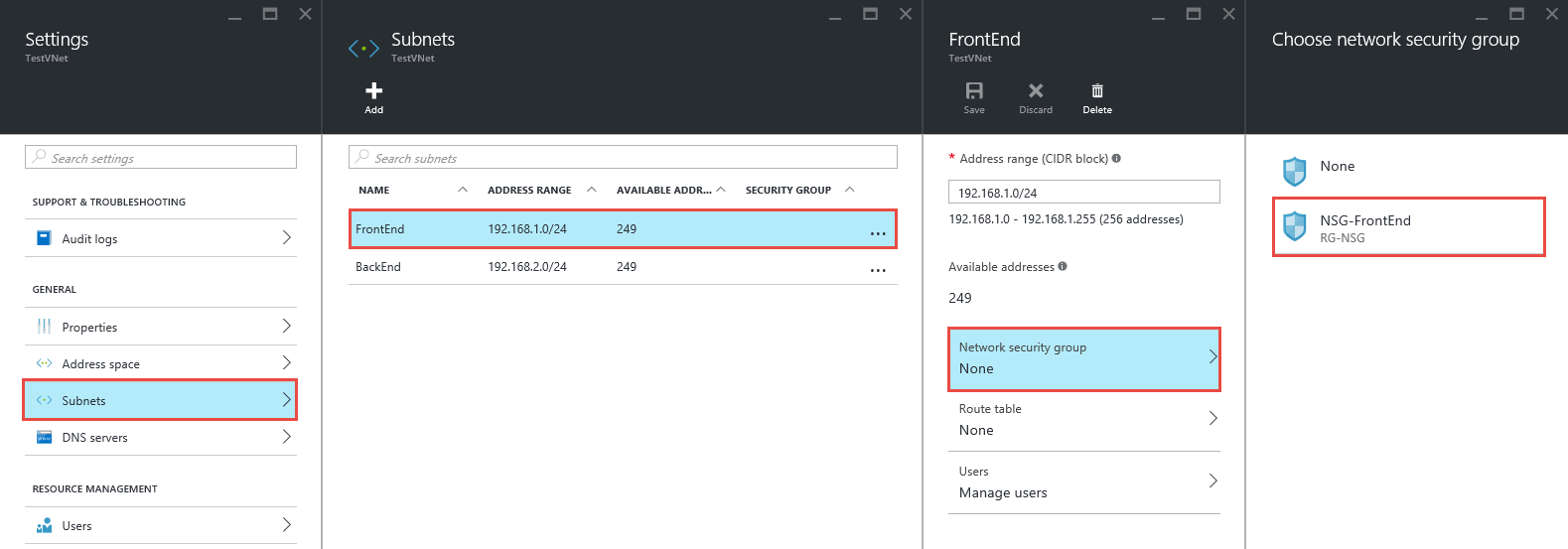
1. Repeat steps to 6 to create an inbound rule named rdp-rule with a priority of 250 allowing access via TCP to port 3389 to any VM from any source.

## Associate the NSG to the FrontEnd subnet

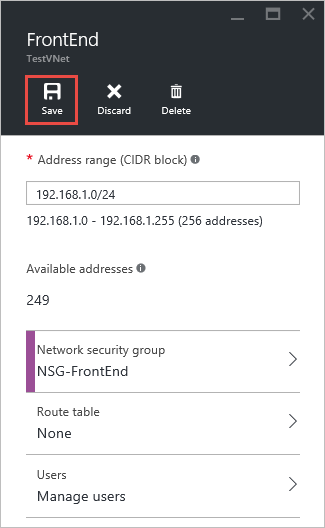
1. Click **Browse >** > **Resource groups** > **RG-NSG**.
2. In the **RG-NSG** blade, click **...** > **TestVNet**.



1. In the **Settings** blade, click **Subnets** > **FrontEnd** > **Network security group** > **NSG-FrontEnd**.



1. In the **FrontEnd** blade, click **Save**.



## Create the NSG-BackEnd NSG

To create the **NSG-BackEnd** NSG and associate it to the **BackEnd** subnet, follow the steps below.

1. Repeat the steps in Create the NSG-FrontEnd NSG to create an NSG named NSG-BackEnd
2. Repeat the steps in Create rules in an existing NSG to create the **inbound** rules in the table below.

| Inbound rule | Outbound rule |
| --- | --- |
| Azure portal - inbound rule | Azure portal - outbound rule |