Networking Lab 2

Network Security Groups

Lab Overview

In this lab, we will see how to create network security groups. Network Security Groups enable restricting flows at a subnet or at a virtual machine’s network interface level. We will create rules and apply at a subnet level. We will also see how application security groups are applied.

Lab Diagram

A close up of a map

Description automatically generated

Create application security groups

An application security group enables you to group together servers with similar functions, such as web servers.

1. Select **+ Create a resource** on the Azure portal.
2. In the **Search the Marketplace** box, enter *Application security group*. When **Application security groups** appears in the search results, select it.
3. Click **+Add**. Enter, or select, the following information:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | Select your subscription |
| Resource group | Select **rg-lab** from the dropdown |
| Name | **mgmt** |
| Location | **West US 2** |

1. Click **Review+Create**.
2. Once validation passes, Click **Create**.
3. Repeat steps 3, specifying the following values:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | Select your subscription |
| Resource group | Select **rg-lab** from the dropdown |
| Name | **web** |
| Location | **West US 2** |

Associate application security group to network interface

1. In the *Search resources, services, and docs* box at the top of the portal, begin typing *virtual machines*. From the search results, select **Virtual machines**.
2. Select virtual machine **vnet1-vm-mgmt1**.
3. Under **Settings** 🡪 **Networking 🡪 Application security groups**, select **Configure the application security groups**, select **mgmt** for **Application security groups**, and then select **Save**.
4. Repeat steps 1-3 for virtual machines **vnet1-vm-web1** and add application group **web**.

Create a network security group

1. In the *Search resources, services, and docs* box at the top of the portal, begin typing *Network security group*. From the search results, select **Network security group**.
2. Click **+Add**. Enter, or select, the following information.

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Subscription | Select your subscription. |
| Resource group | Select**rg-lab** from the dropdown. |
| Name | **nsg1** |
| Location | West US 2 |

1. Click **Review+Create**. Once validation passes, **Create**.

Create security rules

Create a security rule to allow SSH and RDP to the management servers.

1. On the network security groups page, click on the network security group **nsg1** you just created.
2. Go to **Settings** 🡪 **Inbound security rules** and click **+Add**.
3. Enter, or select the following values, accept the remaining defaults, and then select **Add**:

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Destination | Select **Application security group** |
| Destination Application security group | **mgmt** |
| Destination port ranges | Enter 22, 3389 |
| Protocol | Select TCP |
| Priority | Enter 100 |
| Name | allow-mgmt-access |

1. Create another security rule that allows http and https traffic to the **web** application security group.

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Destination | Select **Application security group** |
| Destination Application security group | **web** |
| Destination port ranges | Enter 80,443 |
| Protocol | Select TCP |
| Priority | Enter 120 |
| Name | allow-web |

Associate network security group to subnet

1. On the **Network security groups page**, click on the security group **nsg1**.
2. Under **Settings**, select **Subnets** and then select **+ Associate**, as shown in the following picture:
3. Under **Associate subnet**, select **Virtual network** and then select **vnet1**. Select **Subnet**, select **vnet1-subnet1**, and then select **OK**.
4. Repeat step 3 to associate to subnet **vnet1-subnet2** from **vnet1**.

Verify Network Security group for the virtual machine

1. Go to the virtual machine vnet1-vm-mgmt1.
2. Got to **Settings** 🡪 **Networking**.
3. Check the network security group nsg1 is applied to the subnet vnet-subnet1.
4. You will also see another security group  [vnet1-vm-mgmt1-nsg](https://ms.portal.azure.com/) attached to the network interface of the virtual machine. This was created when you created the VM and assigned Basic network security group as default configuration setting. You can go ahead and disassociate this security group from the network security group as we now have one applied at the subnet level. Note the name of the security group.
5. Click on the network security group attached to the interface.
6. Go to **Settings** 🡪 **Network interfaces**.
7. Click on the three dots **…** on the right and click **Dissociate**.

A screenshot of a cell phone screen with text

Description automatically generated

1. Repeat above steps for each VM created with a basic network security group.

Verify Security rules

 It’s time to see the rules in action.

Connect to the management server from your laptop.

1. From your laptop, do SSH to the management server.
2. SSH to vnet1-vm-mgmt1 using its public IP address.
3. Verify you are successfully able to login.

Which rule enabled ssh access?

Connect to the web server from your laptop.

1. From your laptop, do SSH to the web server.

ssh to vnet1-vm-web1.

Are you able to reach the login prompt?

Which rule was used for this flow?

 Conclusion

We learnt how to configure network security groups and application security groups to protect your compute instances in Azure.

Challenge

Complete additional flows as given in the diagram below to restrict traffic further within your virtual network. Make sure only this traffic is allowed.

A close up of a map

Description automatically generated