**Configure A Network Security in Azure**

**Task 1 - Create a virtual network**

1. From the Azure portal menu, select + Create a resource > Networking > Virtual network, or search for *Virtual Network* in the portal search box.
2. Select Create.
3. On the Basics tab of Create virtual network, enter or select this information:

A screenshot of a computer

Description automatically generated

1. Select the Review + create tab or select the blue Review + create button at the bottom of the page.
2. Select Create.

**Task 2 - Create an application security group**

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

1. From the Azure portal menu, select + Create a resource > Networking > Application security group, or search for Application security group in the portal search box.
2. Select Create.
3. On the Basics tab of Create an application security group, enter or select this information:

|  |  |
| --- | --- |

1. Select the Review + create tab or select the blue Review + create button at the bottom of the page.
2. Select Create.

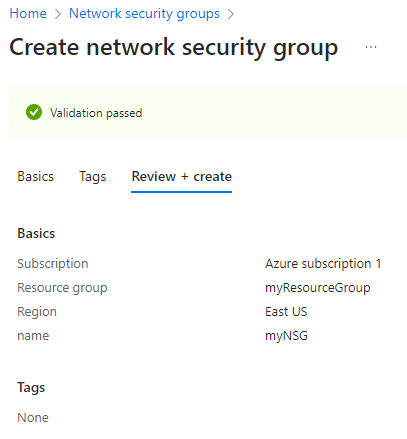
Repeat the previous steps, specifying the following values:  *myAsgMgmtServers*

|  |  |
| --- | --- |
|  |  |

1. Select the Review + create tab or select the blue Review + create button at the bottom of the page.
2. Select Create.

**Task 3 - Create a network security group**

1. From the Azure portal menu, select + Create a resource > Networking > Network security group, or search for *Network security group* in the portal search box.
2. Select Create.
3. On the Basics tab of Create network security group, enter or select this information:



1. Select the Review + create tab or select the blue Review + create button at the bottom of the page.
2. Select Create.

**Task 4 - Associate network security group to subnet**

1. Search for *myNsg* in the portal search box.
2. Select Subnets from the Settings section of myNSG.
3. In the Subnets page, select + Associate:
4. Under Associate subnet, select myVNet for Virtual network.

A white background with black text

Description automatically generated

1. Select default for Subnet, and then select OK.

**Task 5 - Create security rules**

1. Select Inbound security rules from the Settings section of myNSG.
2. In Inbound security rules page, select + Add:
3. Create a security rule that allows ports 80 and 443 to the myAsgWebServers application security group. In Add inbound security rule page, enter or select this information:

| **Setting** | **Value** |
| --- | --- |
| Source | Leave the default of Any. |
| Source port ranges | Leave the default of (\*). |
| Destination | Select Application security group. |
| Destination application security groups | Select myAsgWebServers. |
| Service | Leave the default of Custom. |
| Destination port ranges | Enter *80,443*. |
| Protocol | Select TCP. |
| Action | Leave the default of Allow. |
| Priority | Leave the default of 100. |
| Name | Enter *Allow-Web-All*. |

1. Select Add.
2. Complete steps 3-4 again using this information:

Expand table

| **Setting** | **Value** |
| --- | --- |
| Source | Leave the default of Any. |
| Source port ranges | Leave the default of (\*). |
| Destination | Select Application security group. |
| Destination application security group | Select myAsgMgmtServers. |
| Service | Leave the default of Custom. |
| Destination port ranges | Enter *3389*. |
| Protocol | Select Any. |
| Action | Leave the default of Allow. |
| Priority | Leave the default of 110. |
| Name | Enter *Allow-RDP-All*. |

A screenshot of a computer

Description automatically generated

**Task 6 - Create virtual machines**

1. From the Azure portal menu, select + Create a resource > Compute > Virtual machine, or search for Virtual machine in the portal search box.
2. In Create a virtual machine, enter or select this information in the Basics tab:

Expand table

| **Setting** | **Value** |
| --- | --- |
| Project details |  |
| Subscription | Select your subscription. |
| Resource group | Select myResourceGroup. |
| Instance details |  |
| Virtual machine name | Enter *myVMWeb*. |
| Region | Select (US) East US. |
| Availability options | Leave the default of No infrastructure redundancy required. |
| Security type | Leave the default of Standard. |
| Image | Select Windows Server 2019 Datacenter - Gen2. |
| Azure Spot instance | Leave the default of unchecked. |
| Size | Select Standard\_D2s\_V3. |
| Administrator account |  |
| Username | Enter a username. |
| Password | Enter a password. |
| Confirm password | Reenter password. |
| Inbound port rules |  |
| Select inbound ports | Select None. |

1. Select the Networking tab.
2. In the Networking tab, enter or select the following information:

Expand table

| **Setting** | **Value** |
| --- | --- |
| Network interface |  |
| Virtual network | Select myVNet. |
| Subnet | Select default (10.0.0.0/24). |
| Public IP | Leave the default of a new public IP. |
| NIC network security group | Select None. |

1. Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

A screenshot of a computer

Description automatically generated

A screenshot of a computer error

Description automatically generated

Create the second virtual machine:

A screenshot of a computer error

Description automatically generated

**Associate network interfaces to an Application Security Group**

Add the network interface of each VM to one of the application security groups you created previously:

1. Search for myVMWeb in the portal search box.
2. Select Networking from the Settings section of myVMWeb VM.
3. Select the Application security groups tab, then select Configure the application security groups.
4. In Configure the application security groups, select myAsgWebServers. Select Save.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Task 7 - Test traffic filters**

1. Search for myVMMgmt in the portal search box.
2. On the Overview page, select the Connect button and then select RDP.

A screenshot of a computer

Description automatically generated

1. Select Download RDP file.
2. Open the downloaded rdp file and select Connect. Enter the username and password you specified when creating the VM.
3. Select OK.
4. You may receive a certificate warning during the connection process. If you receive the warning, select Yes or Continue, to continue with the connection.
5. The connection succeeds, because inbound traffic from the internet to the myAsgMgmtServers application security group is allowed through port 3389.