Secure Network traffic using NSGs and ASGs

Use Case:

In this walkthrough task we will create a virtual network and subnet, we will create two application security groups, one for management servers and one for web servers, then create a Network Security group (NSG) and associate that NSG to the subnet. We will then create two inbound network security rules, **allow-rdp-all** and **allow-web-all** traffic.

We will then create two virtual machines, one to represent a management server, and one to represent a web server, associate those virtual machines with their respective application security groups, and then with the network security group (NSG). We will then test the network security rules we have created and applied.

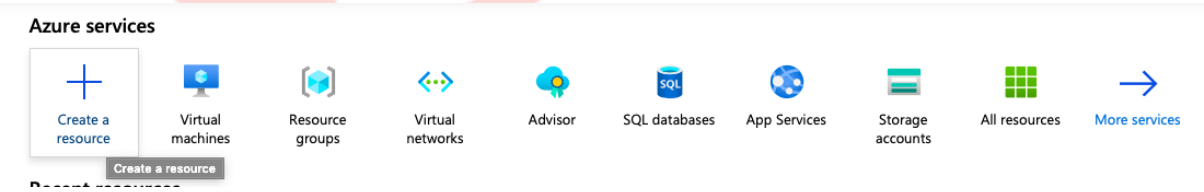
Prerequisites:

You require need an Azure subscription to perform these steps. If you don't have one you can create one by following the steps outlined on the [Create your Azure free account today]() webpage.

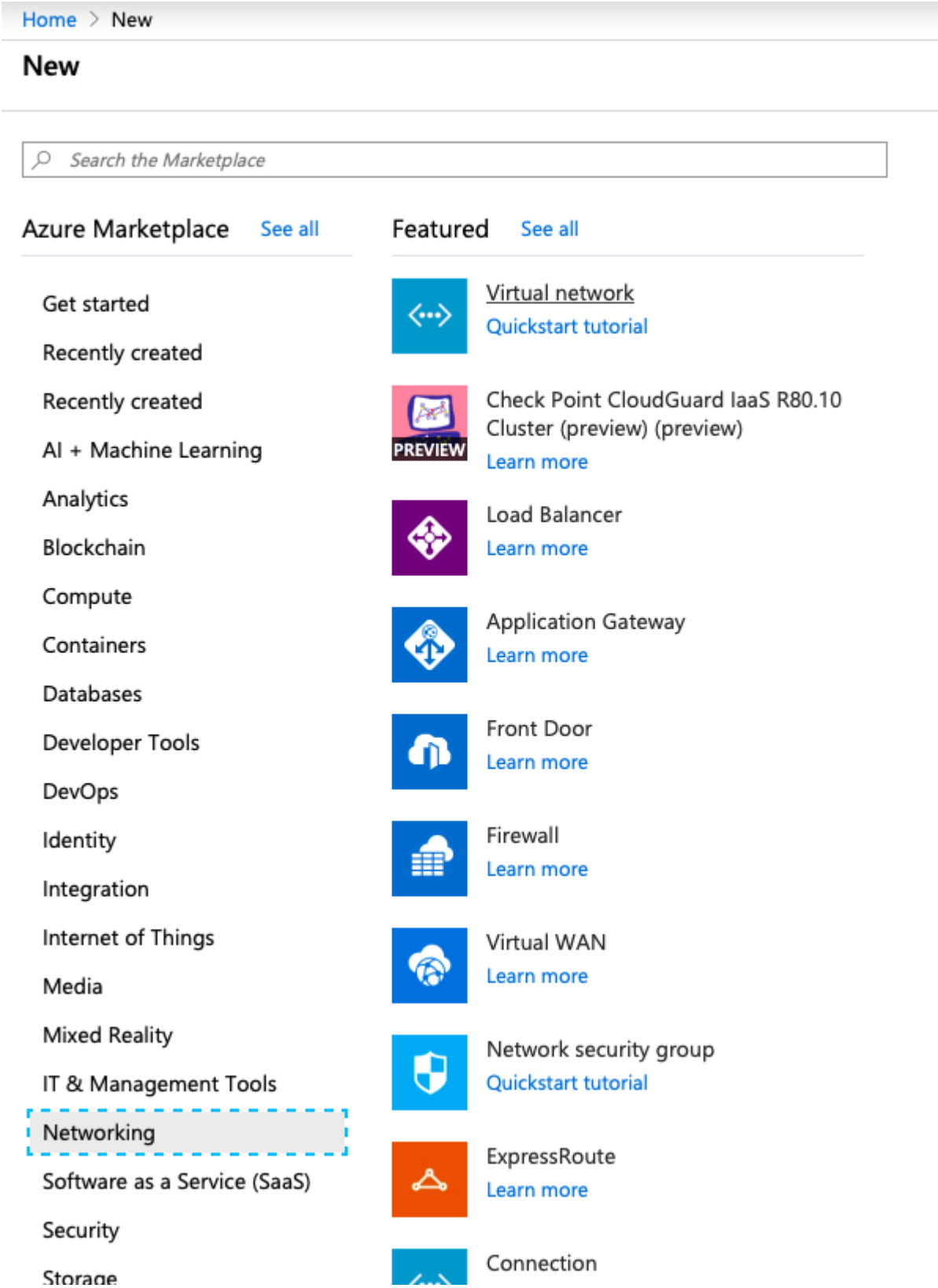
Steps:

Create a virtual network:

1. Sign into the Azure Portal



2. Select **+ Create a resource** on the upper, left corner of the Azure portal, then 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**:

- **Name**: VNET1
- **Address space**: 10.0.0.0/16
- **Subscription** : < select your subscription >
- **Resource group**: < Select **Create new** and enter **netsecrg**. >
- **Location**: (US) East US (or a Datacenter location near you)
- **Subnet**:
- **Name**: subnet1
- **Address range**: 10.0.0.0/24

Home > New > Create virtual network

Create virtual network

Name *

VNET1

Address space *

10.0.0.0/16

10.0.0.0 - 10.0.255.255 (65536 addresses)

The address space '10.0.0.0/16' overlaps with '10.0.0.0/24' in virtual network 'feroz-rg-vnet'.

Add an IPv6 address space

Subscription *

Visual Studio Enterprise – MPN

Resource group *

(New) netsecrg

Create new

Location *

(US) East US

Subnet

Name *

subnet1

Address range *

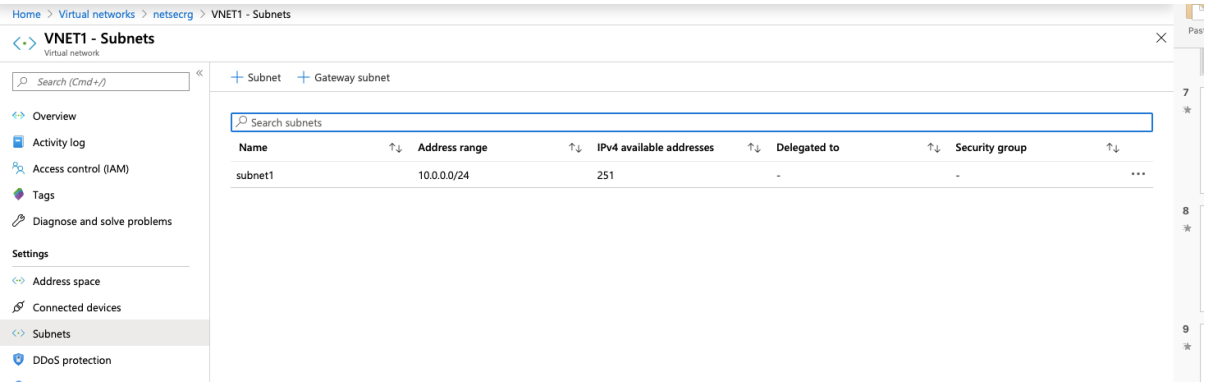
10.0.0.0/24

10.0.0.0 - 10.0.0.255 (256 addresses)

DDoS protection

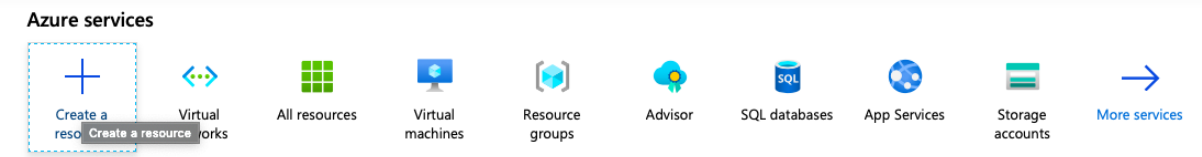
Basic Standard

Create Automation options

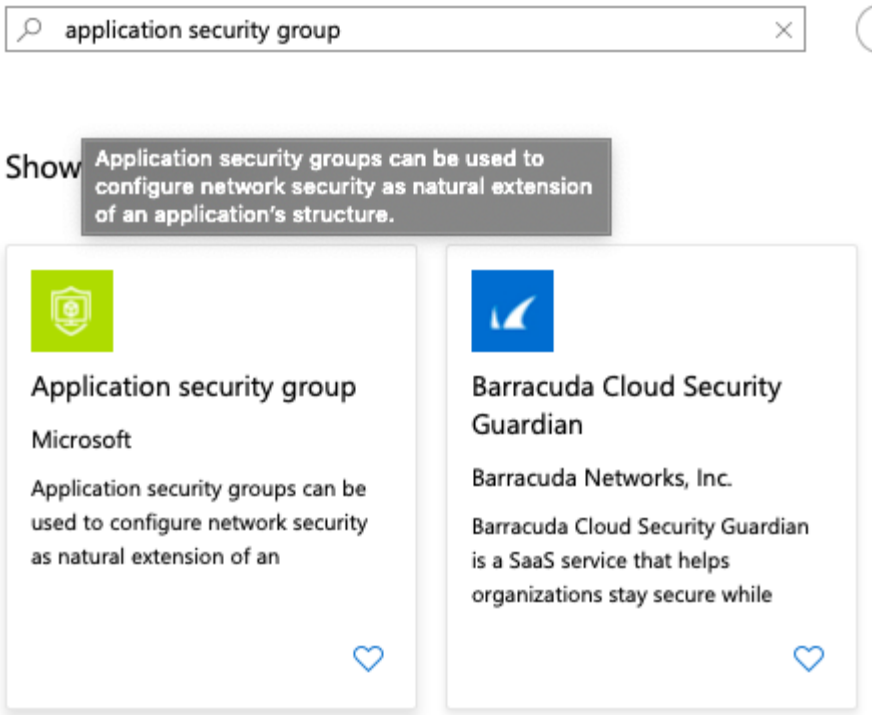


Create two application security groups

1. Select +**Create a resource** on the upper, left corner of the Azure portal.



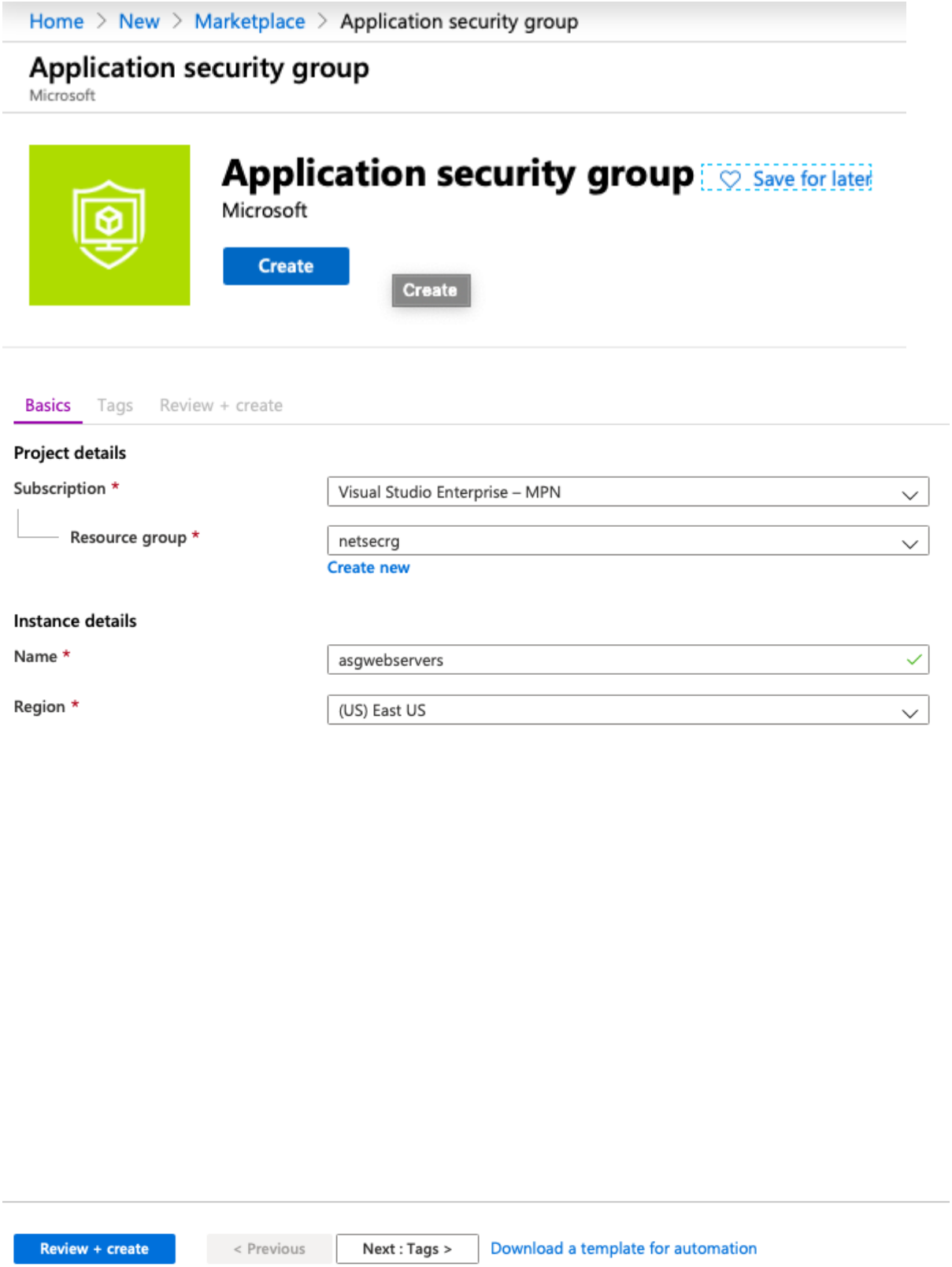
2. In the **Search the Marketplace** box, enter Application security group. When Application security group appears in the search results, select it, select Application security group again under everything and then select Create.

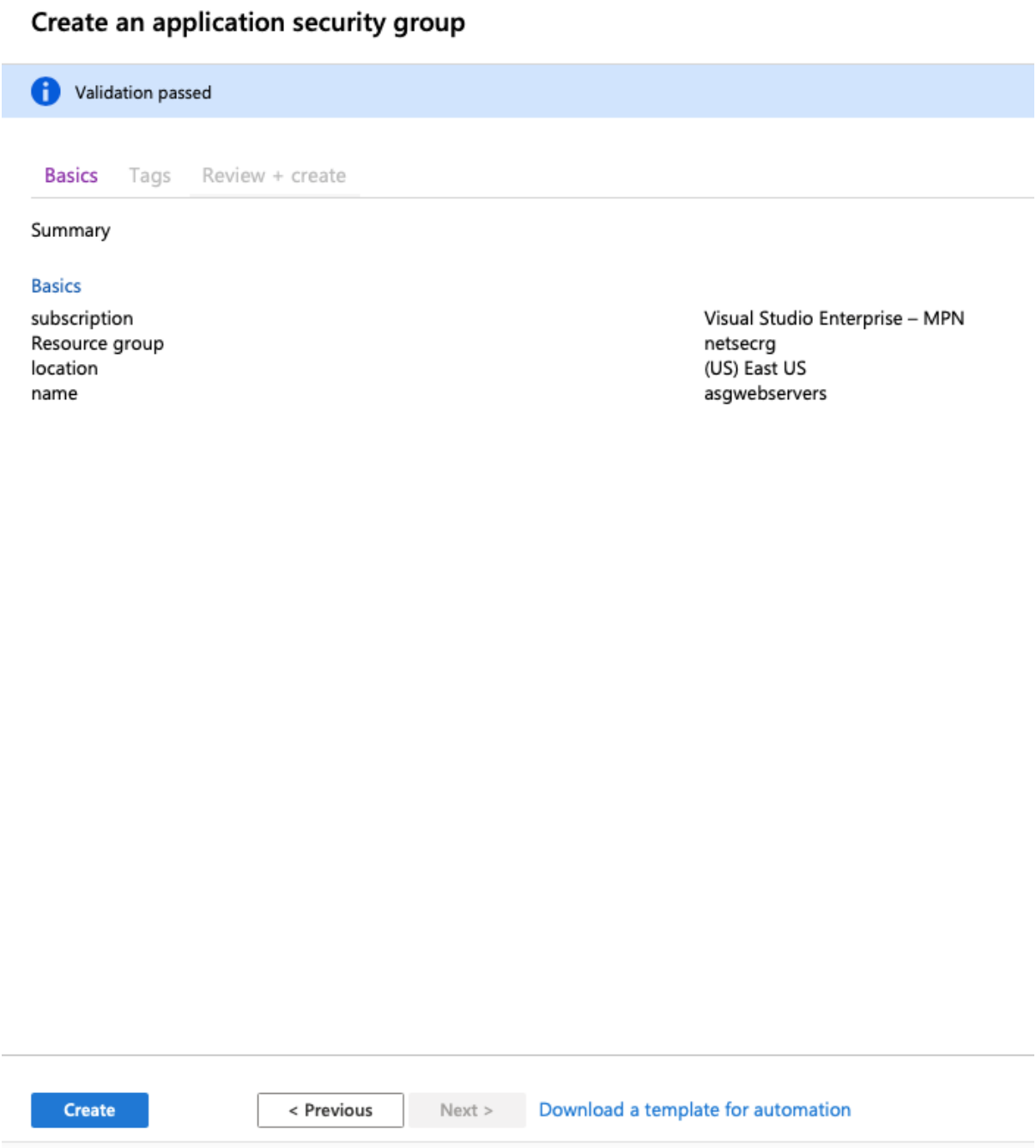


3. Enter the following values then click **Review and Create** followed by **Create**

- **Subscription** : < select your subscription >
- **Resource group**: < **Select existing...** and then select **netsecrg** which you created earlier. >

- **Name**: asgwebservers
- **Region**: (US) East US

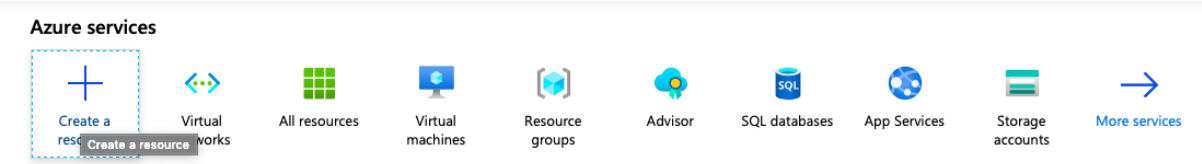




4. Complete steps **1** to **3** again to create another Application security group, specifying the following values:

- **Subscription** : < select your subscription >
- **Resource group**: < **Select existing...** and then select **netsecrg** which you created earlier. >
- **Name**: asgmgmtservers
- **Region**: (US) East US

1. Select +**Create a resource** on the upper, left corner of the Azure portal.



2. In the **Search the Marketplace** box, enter Application security group. When Application security group appears in the search results, select it, select Application security group again under everything and then select Create.

3. Enter the following values then click **Review and Create** followed by **Create**

- **Subscription** : < select your subscription >
- **Resource group**: < **Select existing...** and then select **netsecrg** which you created earlier. >
- **Name**: asgmgmtservers
- **Region**: (US) East US

Basics Tags Review + create

Project details

Subscription * Visual Studio Enterprise – MPN

Resource group * netsecrg

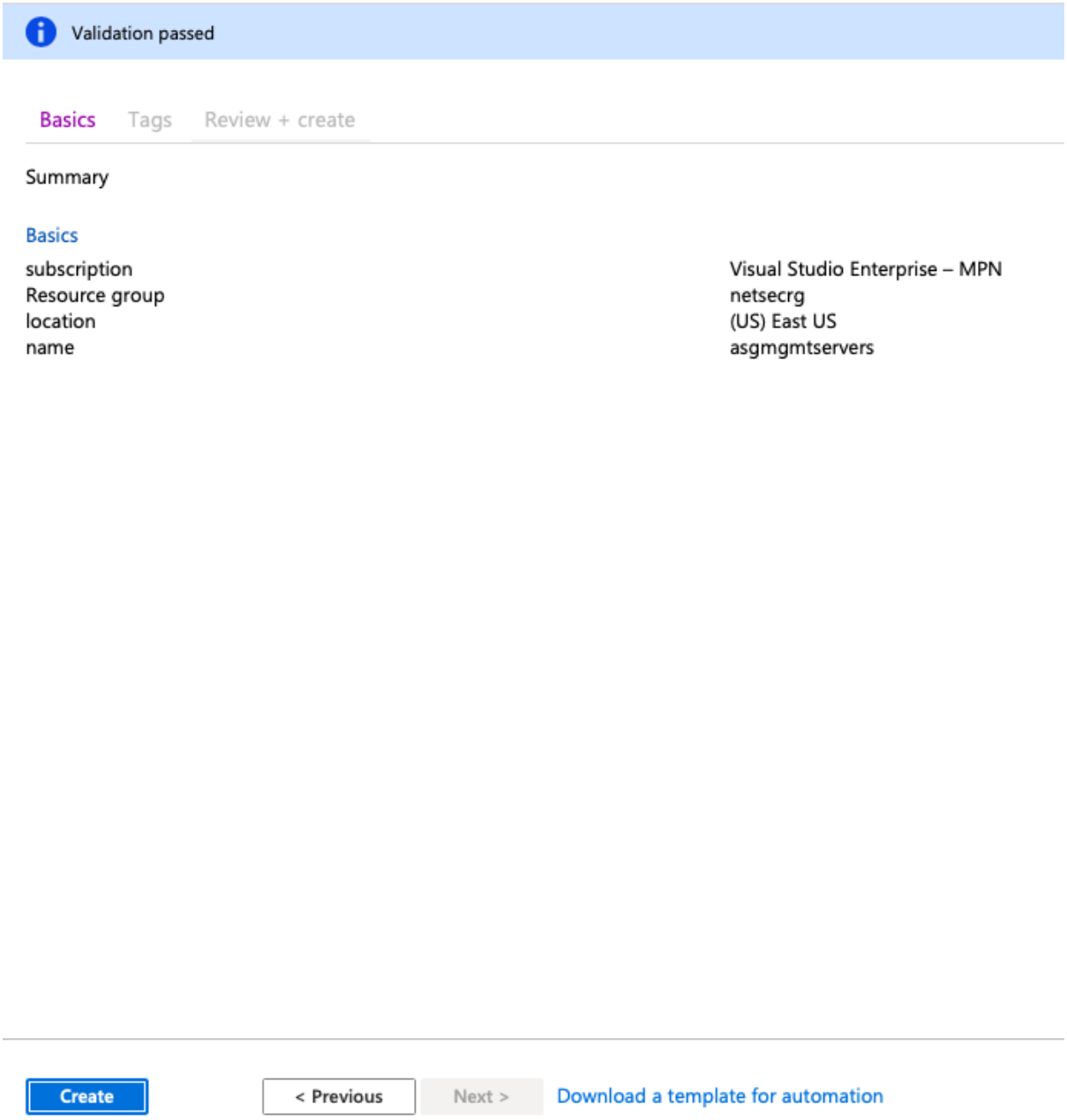
Create new

Instance details

Name * asgmgmtservers

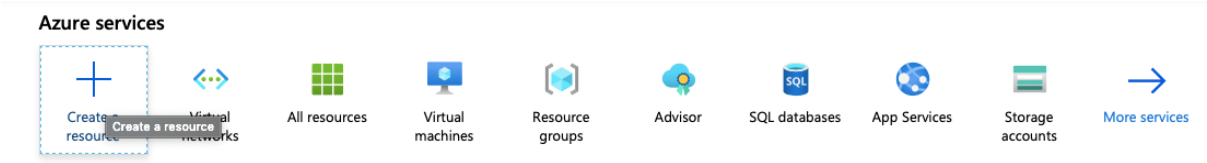
Region * (US) East US

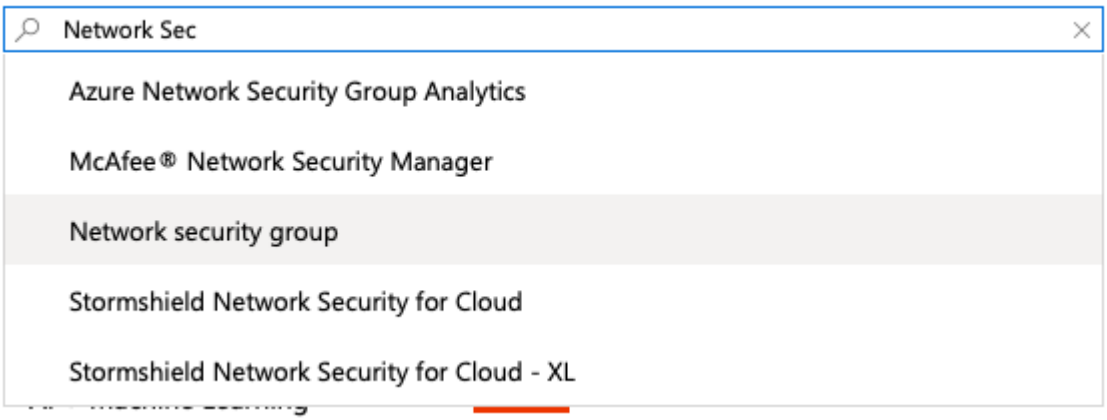
Review + create < Previous Next : Tags > Download a template for automation

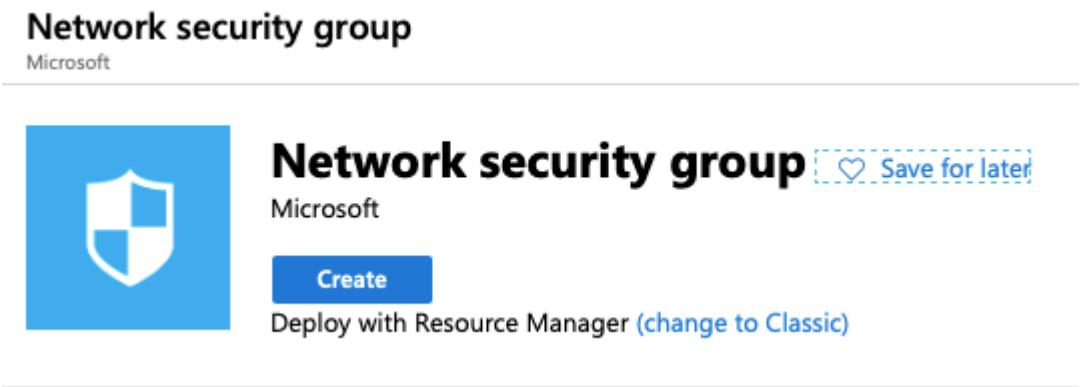


Create a network security group

1. Select **+ Create a resource** on the upper, left corner of the Azure portal, then select **Networking**, and then select **Network security group**







2. Enter, or select, the following information, and then select **Create**:

- **Name**: nsg1
- **Subscription** : < select your subscription >
- **Resource group**: < **Select existing...** and then select **netsecrg** which you created earlier. >
- **Location**: (US) East US

Create network security group

Basics | Tags | Review + create

Project details

Subscription * : Visual Studio Enterprise – MPN

Resource group * : netsecrg

Create new

Instance details

Name * : nsg1

Region * : (US) East US

Review + create | < Previous | Next : Tags > | Download a template for automation

Create network security group

Validation passed

Basics Tags Review + create

Basics

Subscription	Visual Studio Enterprise – MPN
Resource group	netsecrg
Region	(US) East US
name	nsg1

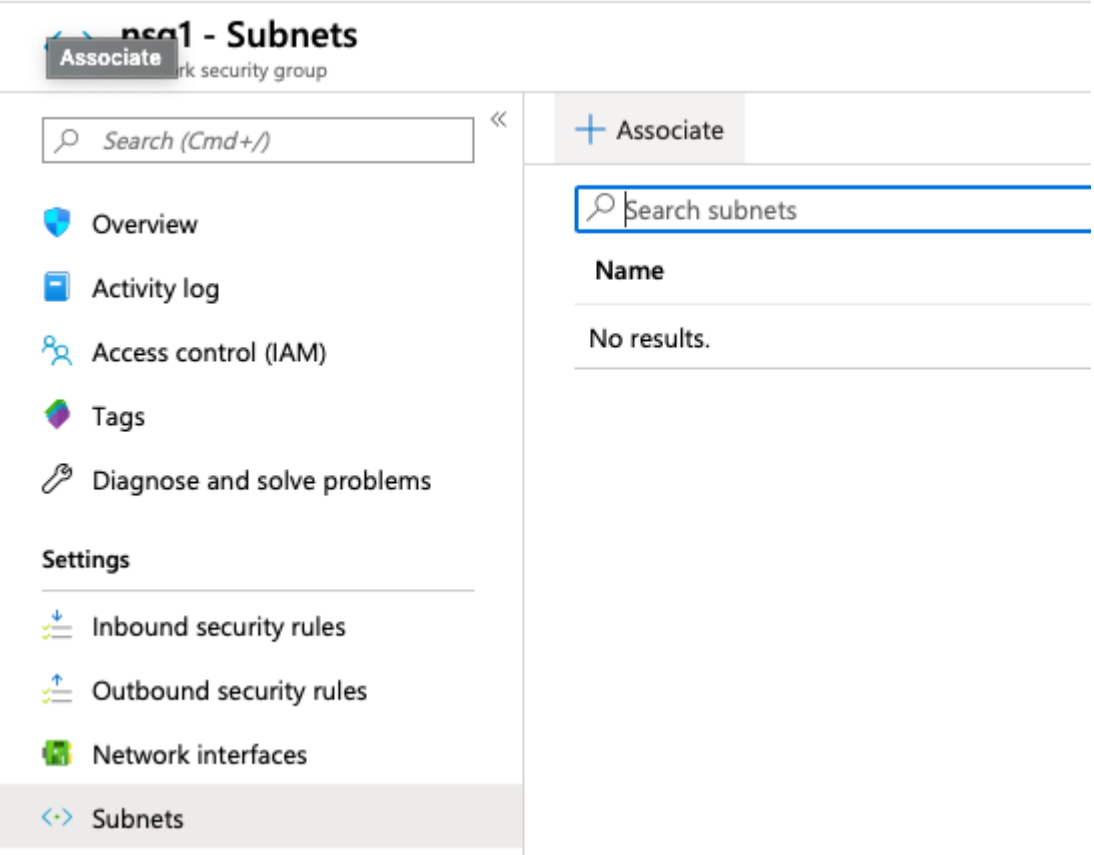
Tags

None

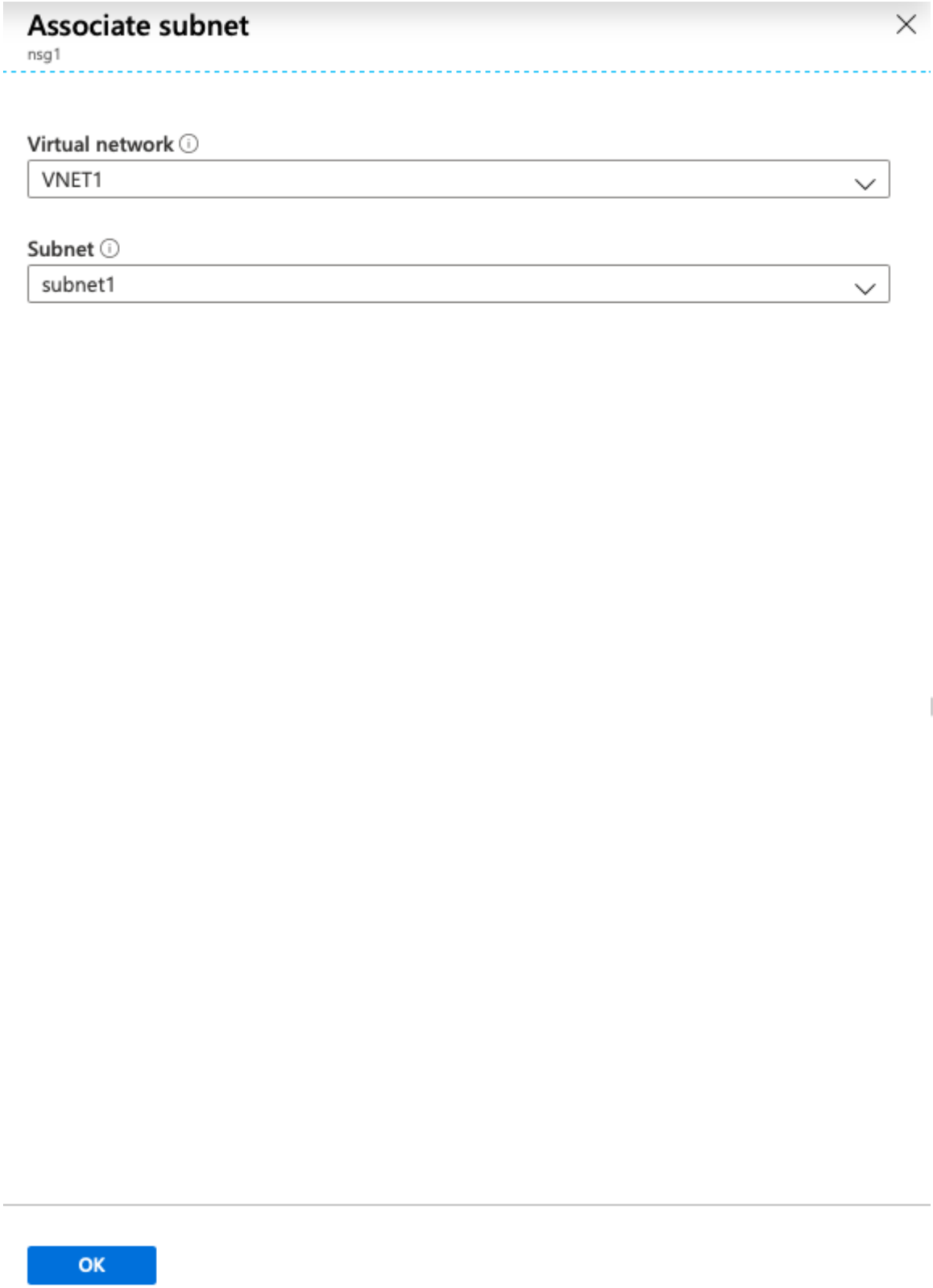
Create < Previous Next > Download a template for automation

Associate the network security group to a subnet

1. Open the Network security group you just created, nsg1, Under SETTINGS, select Subnets and then select + Associate

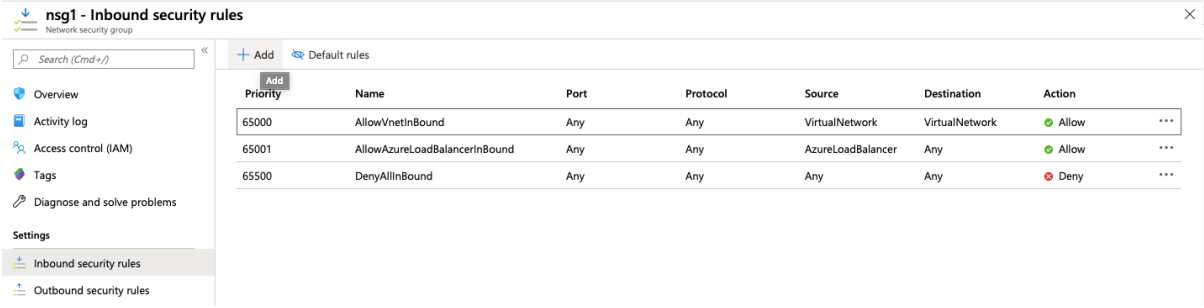


2. Open the Network security group you just created, **nsg1**, Under **SETTINGS**, select **Subnets** and then select **+ Associate**



Create security rules

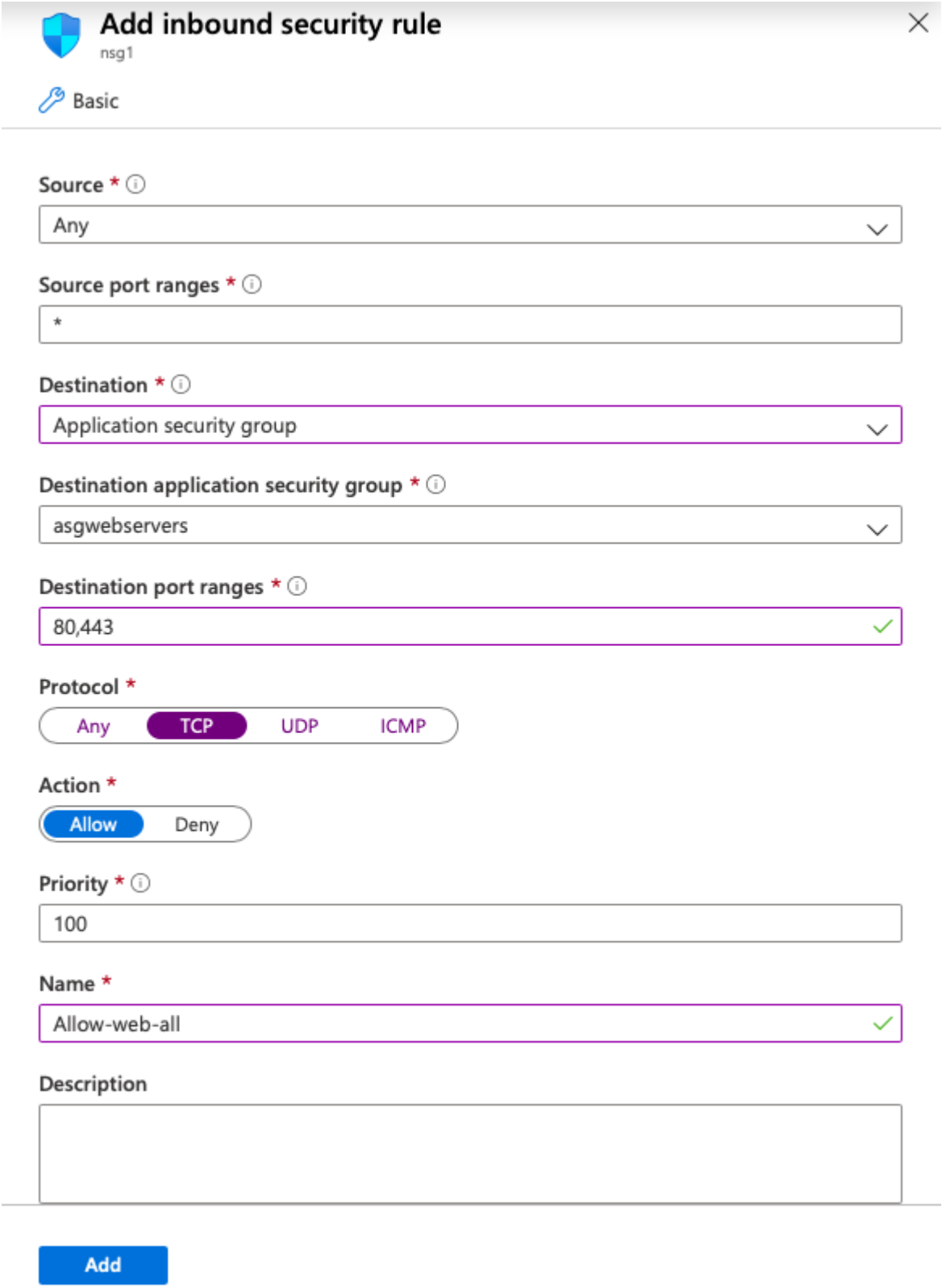
1. Still in the Network Security group, Under **SETTINGS**, select **Inbound security rules** and then select **+ Add**.



2. Create a security rule that allows ports **80** and **443** to the **AsgWebServers** application security group. Under Add inbound security rule, enter, or select the following values, accept the remaining defaults, and then select **Add** when finished.

- **Source**: Any
- **Source port ranges**: *
- **Destination**: Application security group
- **Destination application security group**: asgwebservers
- **Destination port ranges**: 80,443
- **Protocol**: TCP
- **Action**: Allow
- **Priority**: default
- **Name**: Allow-Web-All

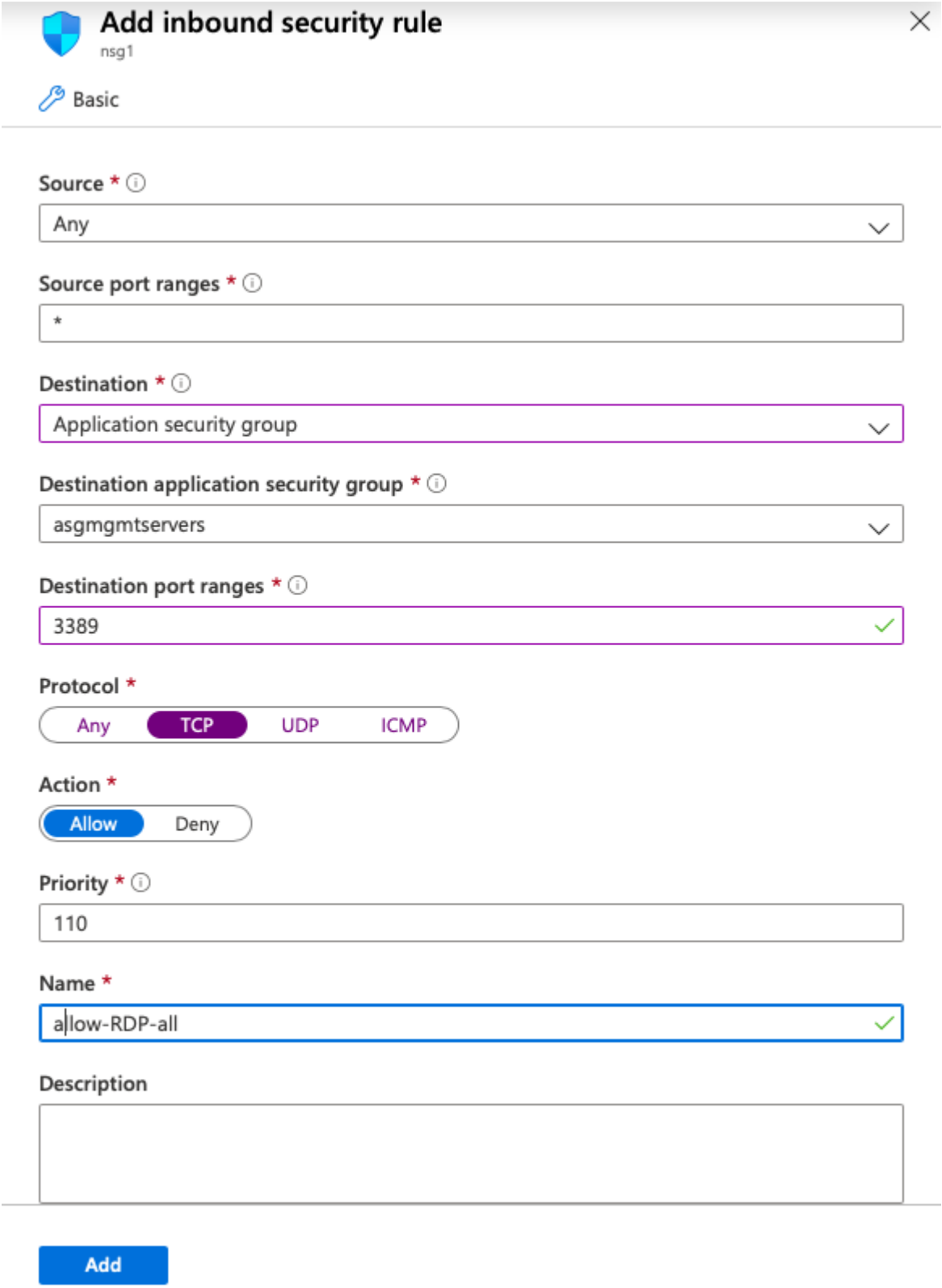
This allows us to connect to the web server from the internet over ports 80 and 443 only.



3. Create another inbound security rule by repeating steps **1** and **2** again, using the following values:

- **Source**: Any
- **Source port ranges**: *

- **Destination**: Application security group
- **Destination application security group**: asgmgmtservers
- **Destination port ranges**: 3389
- **Protocol**: TCP
- **Priotity**: 110
- **Name**: Allow-RDP-All


Add inbound security rule
nsg1
Basic
Source *
Any
Source port ranges *
*
Destination *
Application security group
Destination application security group *
asgmgmtservers
Destination port ranges *
3389
Protocol *
Any
TCP
UDP
ICMP
Action *
Allow
Deny
Priority *
110
Name *
allow-RDP-all
Description
Add

Note:

- The port **3339**, the rdp port, is exposed to the internet for the VM that is assigned to the **asgmgmtservers** application security group. For production environments, instead of exposing port 3389 to the internet, it's recommended that you connect to Azure resources that you want to manage using a VPN or private network connection.
- Also, we designated the value **Any** for source to indicate access from the internet.

4. Review the rules you created. Your list should look like the list in the following picture:

Create virtual machines

1. In the Azure Portal, click on the **Cloud Shell** icon in the top right hand corner.

2. The **Cloud Shell** is launched in the bottom of the browser window.

3. Run the below Azure CLI command to create the first virtual machine, this command will run fine in either **powershell** *or* **bash** console. You can copy and paste the command from below directly into the Cloud Shell console and press **Enter** to run it.

```cli
az vm create `
--name vmmgmt1 `
--resource-group netsecrg `
--image Win2019Datacenter `
--location eastus `
--vnet-name VNET1 `
--subnet subnet1 `
--nsg nsg1 `
--asg asgmgmtservers `
--admin-username azureuser `
--admin-password Password0134!
```

```
Microsoft Azure        Search resources, services, and docs (G+/)        feroz@codesizzler.info
                                                                         JUI TECHNOLOGIES PRIVATE LIM...
PowerShell
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell


MOTD: Switch to PowerShell from Bash: pwsh

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
Azure:/
PS Azure:\> az vm create --name vmmgmt1 --resource-group netsecrg --image Win2019Datacenter --location eastus --vnet-name VNET1 --subnet subnet1 --nsg nsg1 --
asg asgmgmtservers --admin-username demouser --admin-password demo@pass123
{
  "fqdns": "",
  "id": "/subscriptions/[redacted]/resourceGroups/netsecrg/providers/Microsoft.Compute/virtualMachines/vmmgmt1",
  "location": "eastus",
  "macAddress": "00-0D-3A-53-B7-FC",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "52.186.67.15",
  "resourceGroup": "netsecrg",
  "zones": ""
}
```

Note: The command will take two to three minutes to complete and should run successfully. Do not continue to the next step until the VM is deployed.

3. Create the second virtual machine by running the following command in the same cloud shell console in the browser window.

```cli
az vm create `
--name vmweb1 `
--resource-group netsecrg `
--image Win2019Datacenter `
--location eastus `
--vnet-name VNET1 `
--subnet subnet1 `
--nsg nsg1 `
--asg asgwebservers `
--admin-username azureuser `
--admin-password Password0134!
```

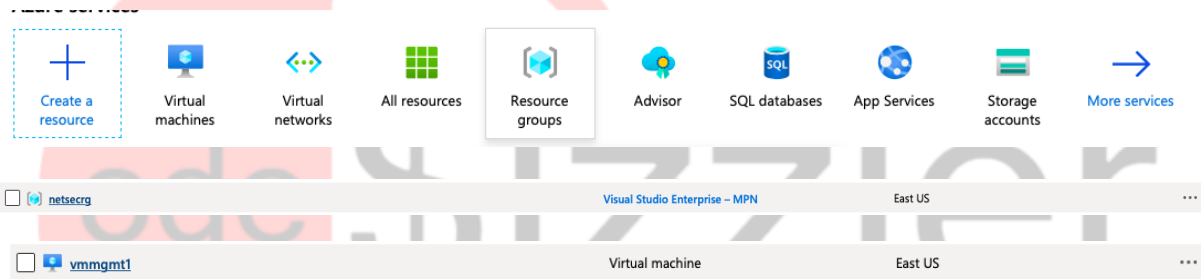
```
PS Azure:\> az vm create --name vmweb1 --resource-group netsecrg --image Win2019Datacenter --location eastus --vnet-name VNET1 --subnet subnet1 --nsg nsg1 --a
sg asgwebservers --admin-username demouser --admin-password demo@pass123
{
  "fqdns": "",
  "id": "/subscriptions/[redacted]/resourceGroups/netsecrg/providers/Microsoft.Compute/virtualMachines/vmweb1",
  "location": "eastus",
  "macAddress": "00-0D-3A-54-F1-F8",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.5",
  "publicIpAddress": "52.226.66.146",
  "resourceGroup": "netsecrg",
  "zones": ""
}
Azure:/
```

Note: Items to note from the deployment.

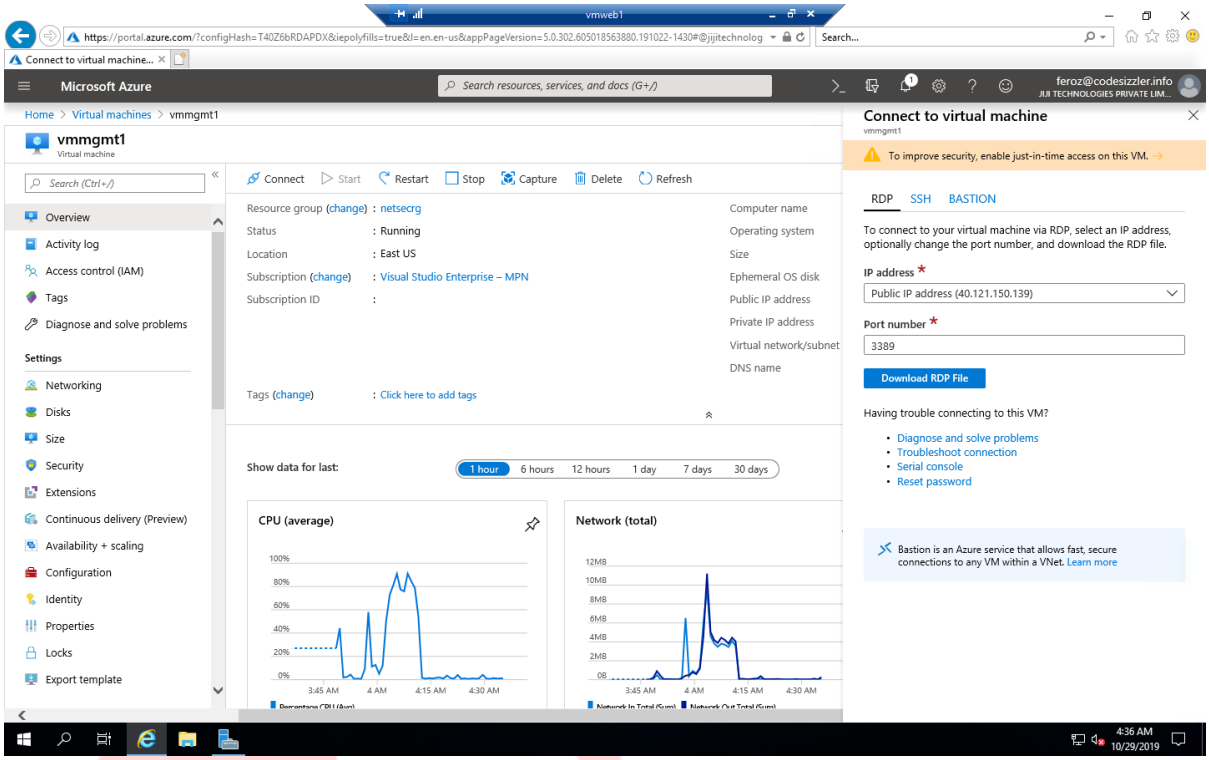
- We created a network interface for each VM, and attached the network interface to the VM.
- Both network interfaces are in Virtual network **VNET1** and its subnet **subnet1**.
- **subnet1** is part of the Network Security Group, **nsg1**, so as such the **nsg1** security rules are applied to the two virtual machines.
- **vmmgmt1** has been associated with the application security group **asgmgmtservers**
- **- vmweb1** has been associated with the application security group **asgwebservers***

Test traffic filters

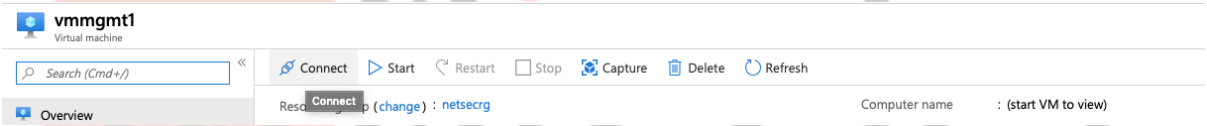
1. In the Azure Portal, go to your resource group, i.e. **netsecrg**, open the **vmmgmt1** virtual machine and connect to it by clicking on the **Connect** button.



2. In the **Connect to virtual machine** blade select **Download RDP File** and click to open the rdp file when prompted to do so.

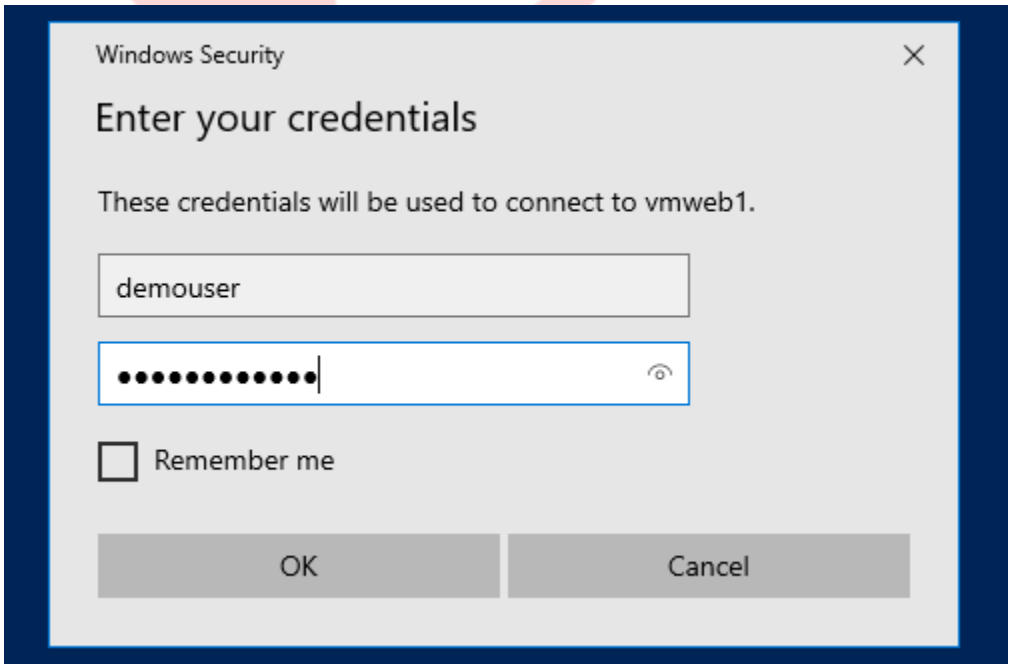


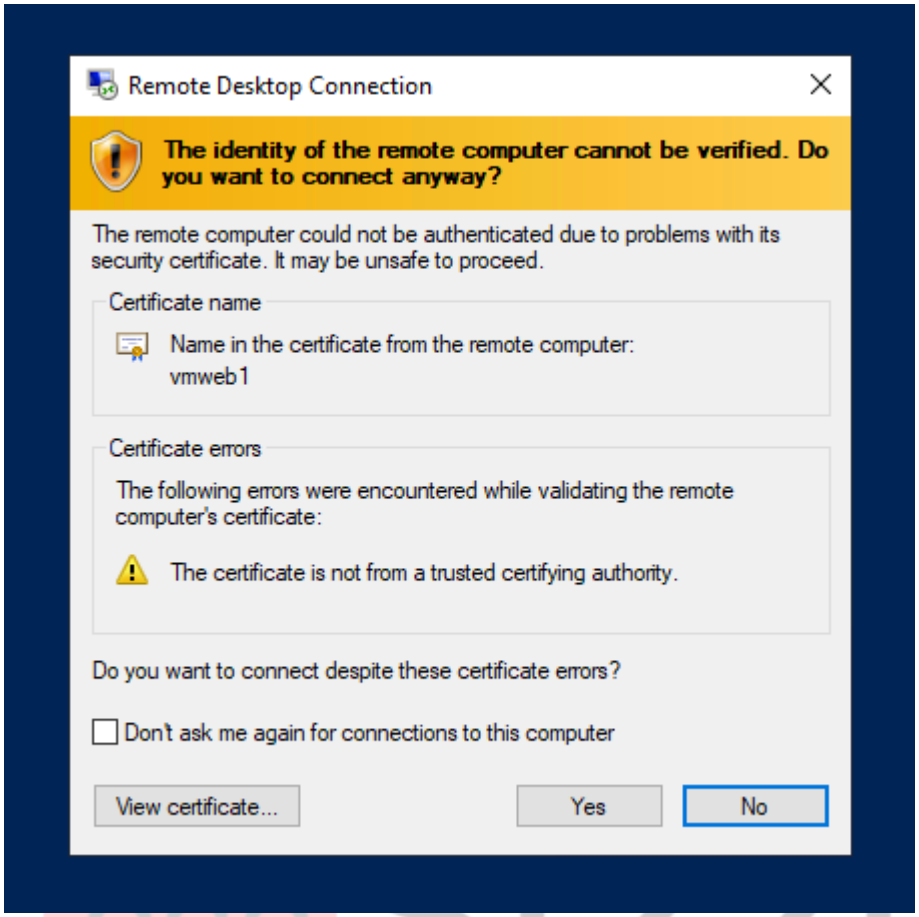
3. In the **Remote Desktop Connection** dialogue select **Connect**.



4. In the **Windows Security > Enter your credentials** dialogue select **More Choices.**

5. Select use a different account and enter the user name and password you specified when creating the VM, as below, then click **OK**.





Note:

- 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.
- The connection succeeds, because port 3389 is allowed inbound connections from the internet to the **asgmgmtservers** application security group, i.e. the **vmmgmt1** virtual machine is in the **VNET1** virtual network and the subnet **subnet1** which has those security rules associated with it as defined by the Network Security group **nsg1**.

6. From within the **vmmgmt1** virtual machine we will now connect via rdp to the **vmweb1** virtual machine. Still within the remote desktop connection to **vmmgmt1**, go to the start menu, type PowerShell, then locate and launch **Powershell**, by right clicking it and choosing **Run as Administrator.**

7. We will now install **Internet Information Service (IIS)** on the **vmweb1** to allow it function as a webserver. Return to the remote desktop connection to **vmweb1** virtual machine and open a **Powershell** prompt by clicking on the start button, typing **Powershell**, the right clicking it and choosing **Run as administrator** 12. In the resultant Powershell console prompt, install Microsoft **Internet.**

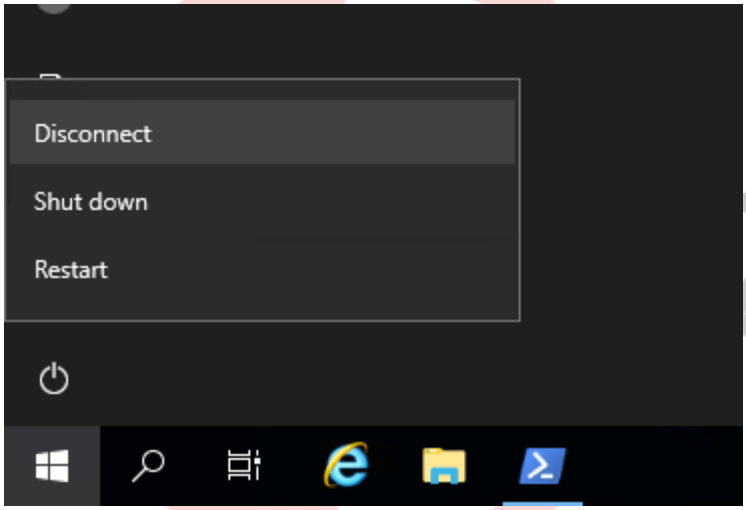
Information Service (IIS) on the **vmweb1** virtual machine, by running the following command within the PowerShell session.

```

Install-WindowsFeature -name Web-Server -IncludeManagementTools

```

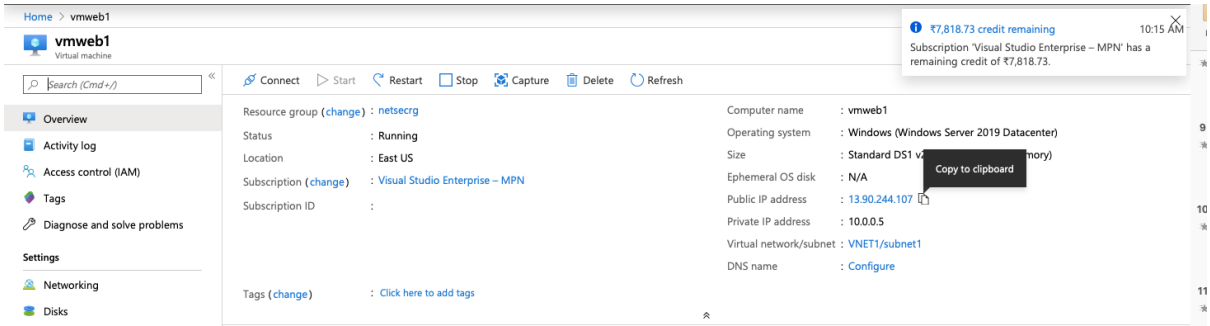
```
PS C:\Users\demouser> Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

8. The installation should complete successfully

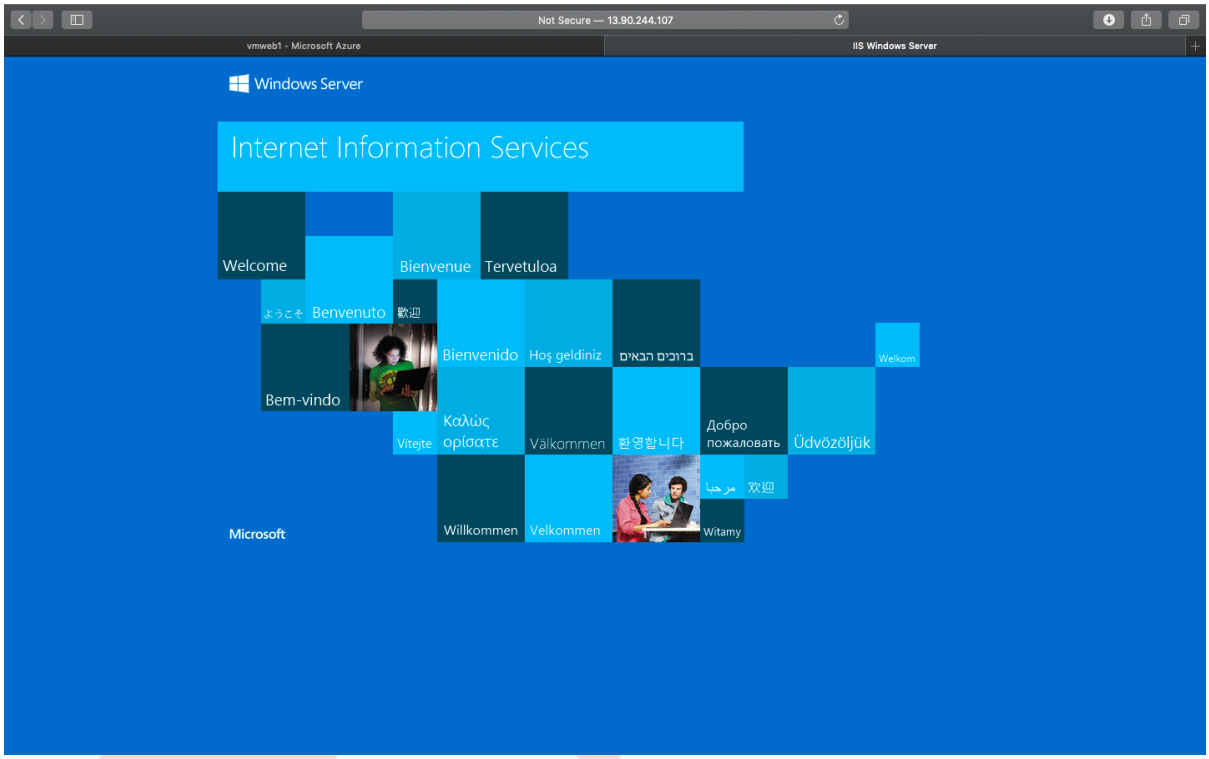
9. Disconnect from the **vmweb1** virtual machine, which leaves you in the **vmmgmt1** remote desktop connection, then also disconnect from the **vmmgmt1** virtual machine.



10. In the Azure portal open the **vmweb1** , go to **Overview** and note the **Public IP address** for the virtual machine. The address shown in the following picture is 13.90.244.107, but your address will be different:



11. From your local machine access the **vmweb1** web server from the internet by opening an internet browser on your computer. You see the IIS welcome screen.


Not Secure — 13.90.244.107
vmweb1 - Microsoft Azure
IIS Windows Server
Windows Server
Internet Information Services
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歓迎
Bienvenido
Hoş geldiniz
ברוכים הבאים
Welkom
Bem-vindo
Καλώς ορίσατε
Vítejte
Välkommen
환영합니다
Добро пожаловать
Üdvözöljük
مرحبا
欢迎
Willkommen
Velkommen
Witamy
Microsoft