Implement an Azure Firewall using Azure Portal

Use Case:

From a network architecture perspective, we will create a single Virtual Network (VNET) which will contain three subnets. The three subnets will be

- AzureFirewallSubnet: Contains Azure Firewall and all workload server traffic will be routed through Azure Firewall.
- Workload-SN: Contains the Workload server i.e. a server where a production application would run. We create a default route so that this subnet's network traffic is configured to go through the firewall. The workload server will not have a publicly accessible connection available to it and will only be accessible via a *Jump server*(*Jump box*). We will configure Azure Firewall to allow the workload server to access DNS servers over port 53 to allow it access web sites on the internet.
- Jump-SN: Contains a *Jump server* which has a public IP address that you can connect to using Remote Desktop. From there, you can then connect to (using another Remote Desktop) the workload server.

Prerequisites:

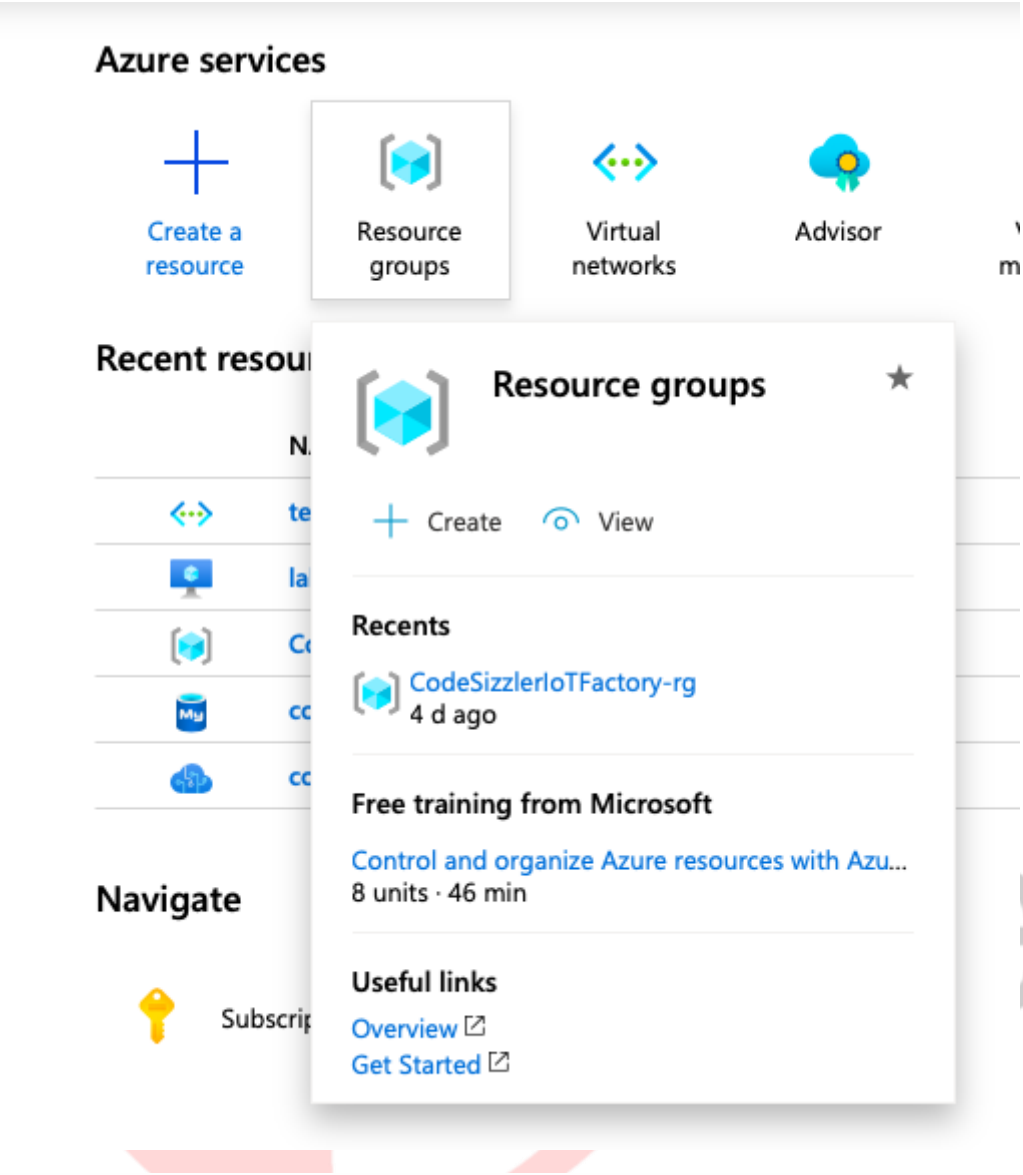
You require need an Azure subscription to perform these steps. If you don't have one you can create one by following the steps outlined on the Create your Azure free account today webpage.

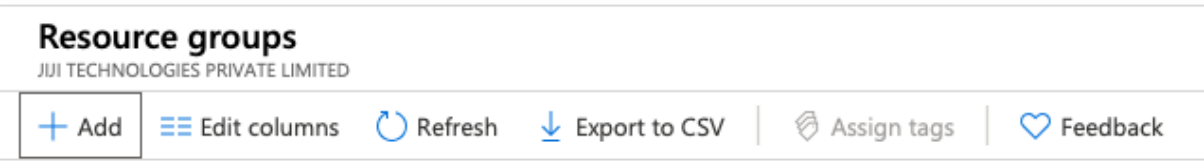
Steps:

Create Resource group

1. Sign in to the Azure portal at https://portal.azure.com

2. On the Azure portal home page, click **Resource groups** > **Add** and use the following details and click **Review and Create** and then **Create**.





- **Subscription**: < select your own subscription >
- **Resource group**: az900-rg
- **Region**: < select a Datacenter location nearest to you. Note: All subsequent resources that you create must be in the same location. >

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

Project details

Subscription * Visual Studio Enterprise – MPN

Resource group * az900-rg

Resource details

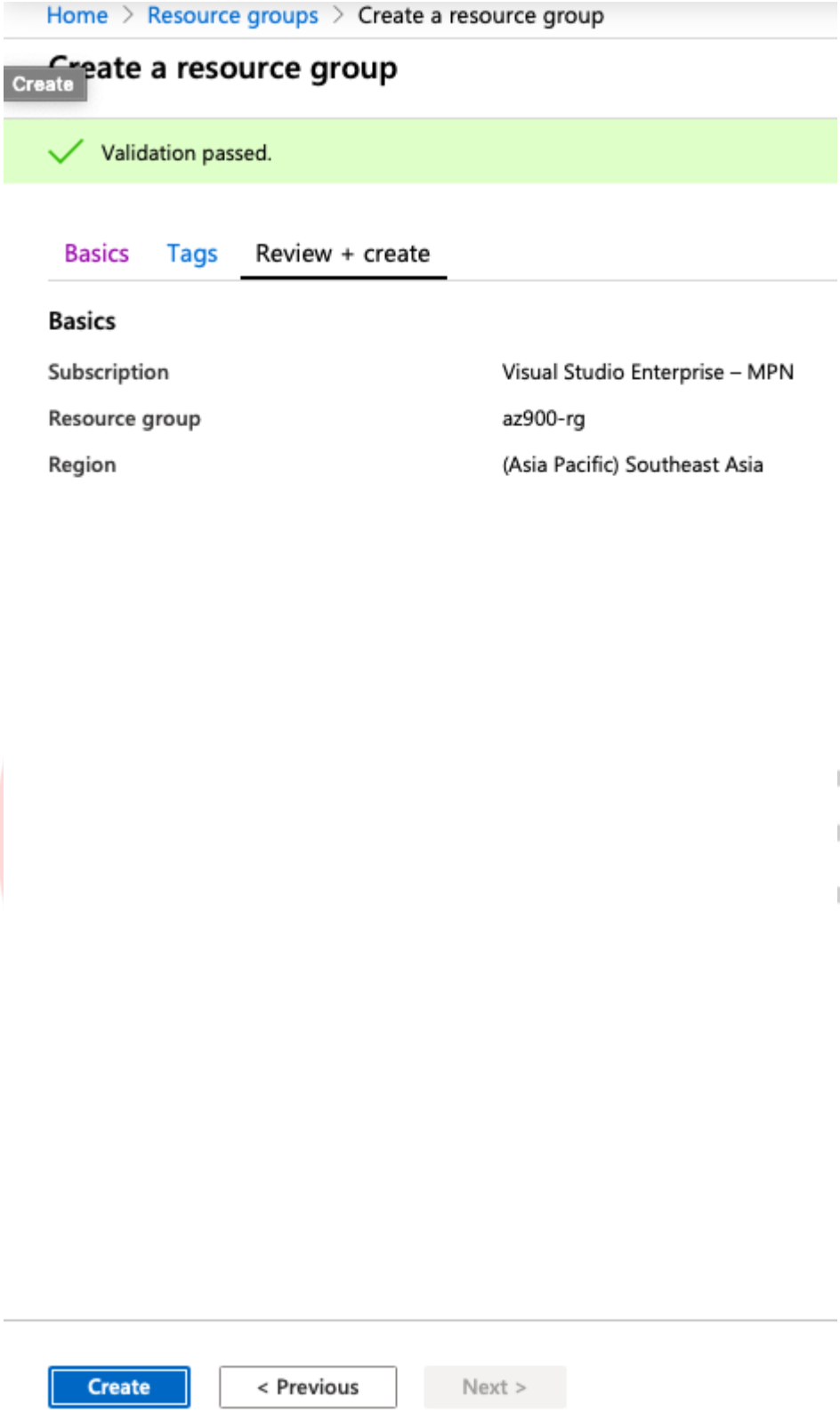
Region * Southeas

Recommended

(Asia Pacific) Southeast Asia

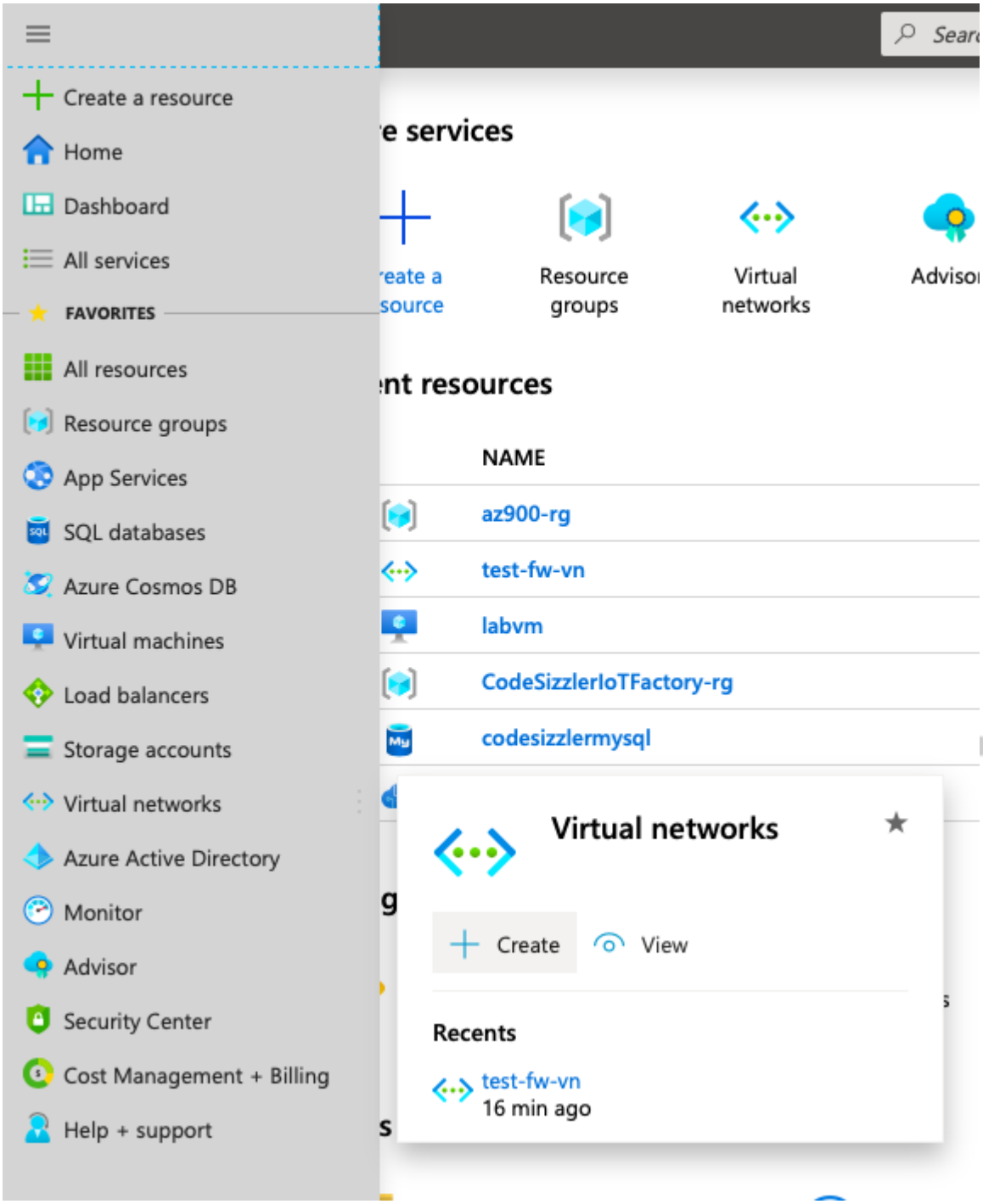
Other

Click on create button.



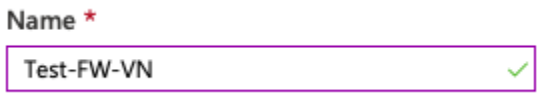
Create a VNET

1. From the Azure portal home page, click **All services** > **Networking** > **Virtual networks**.



2. Click **Add** and use the following details, leaving any other values as their default a click **Create** when finished

- **Name**: Test-FW-VN



- **Address space**: 10.0.0.0/16

Address space * ⓘ

10.0.0.0/16

10.0.0.0 - 10.0.255.255 (65536 addresses)

- **Subscription** : < select your subscription >

Subscription *

Visual Studio Enterprise – MPN

- **Resource group**: < select resource group created earlier az900-rg >

Resource group *

az900-rg

Create new

- **Location**: < select the same location that you used previously >

Location *

(Asia Pacific) Southeast Asia

- **Subnet>**
- **Name**: AzureFirewallSubnet (The firewall will be in this subnet, and the subnet name must be AzureFirewallSubnet).
- **Address range**: 10.0.1.0/24

Subnet

Name *

AzureFirewallSubnet

Address range * ⓘ

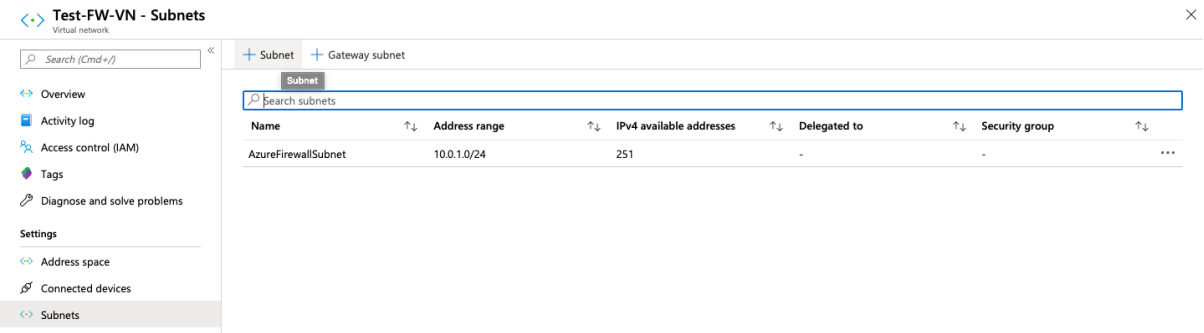
10.0.1.0/24

10.0.1.0 - 10.0.1.255 (256 addresses)

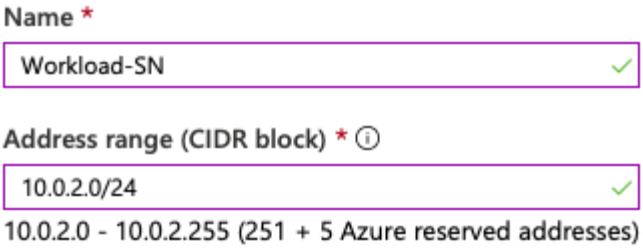
Create additional subnets

Next we will create some additional subnets, into which we will subsequently place two virtual machines.

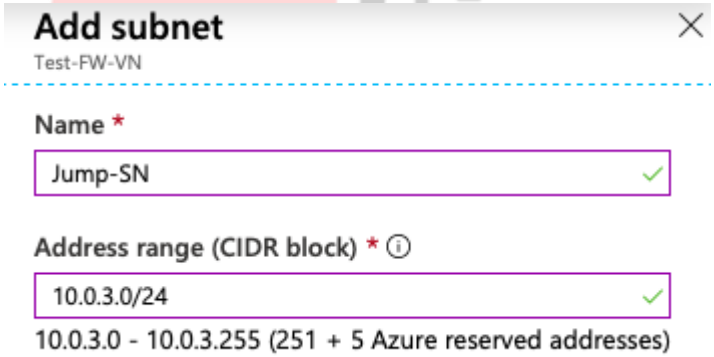
1. On the Azure portal home page, click **Resource groups** > **az900-rg**.
2. Click the **Test-FW-VN** virtual network.
3. Click **Subnets** > **+ Subnet** and use the following details, leaving the remaining items at their default values and click **OK** when completed



- **Name**: Workload-SN
- **Address range**: 10.0.2.0/24



4. Create another subnet by repeating steps 1-3 above, using the values
   - **Name**: Jump-SN
   - **Address range**: 10.0.3.0/24



Create a virtual machine in each subnet

Now we will create two virtual machines and place them in the two additional subnets created in the previous section, one for the Jump-SN subnet, and one for the Workload-SN subnet.

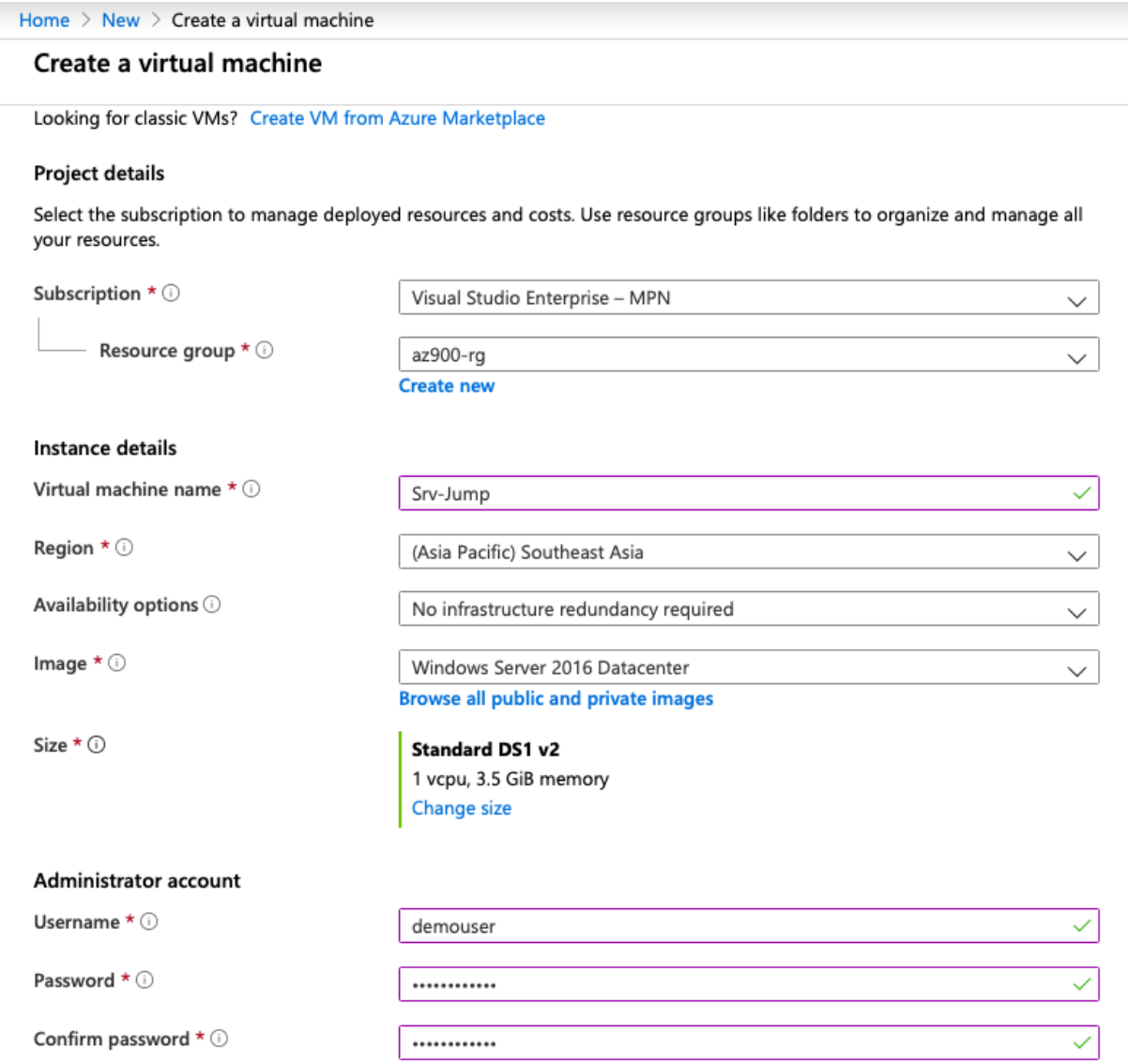
1. On the Azure portal, click **Create a resource**.

2. Click **Compute** and then select **Windows Server 2016 Datacenter** in the Featured list.

Windows Server 2016 Datacenter
Quickstart tutorial

3. Enter these values for the virtual machine, accepting the default values for items not listed below. When finished click **Review + Create**, then click **Create**

- **Basic:**
- **Subscription**: < select your subscription >
- **Resource group:** Test-FW-RG < the resource group you created earlier >
- **Virtual machine name:** Srv-Jump
- **Region**: < The region you selected earlier >
- **Size** – Standard DS1 V2
- **Username**: demouser
- **Password**: demo@pass123



- **Public inbound ports:** RDP (3389).

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ ○ None ◉ Allow selected ports

Select inbound ports * RDP (3389)

- **Disks:**
- **Disk options** – OS disk type: Premium SSD

Disk options

OS disk type * ⓘ Premium SSD

- **Networking:**
- Virtual Network: Test-FW-VN
- Subnet: Jump-SN
- Public IP: click Create new then type Srv-Jump-PIP for the public IP address name and click OK.

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ Test-FW-VN
Create new

Subnet * ⓘ Jump-SN (10.0.3.0/24)
Manage subnet configuration

Public IP ⓘ (new) Srv-Jump-ip
Create new

- **Management:**
- Boot diagnostics: Off

Monitoring

Boot diagnostics ⓘ ○ On ◉ Off

- Click on create button.

4. While the virtual machine is being created, repeat steps 1-3 above to create another virtual machine with the following settings:

Azure services

Create a resource | Resource groups | Virtual networks | Advisor | Virtual machines | SQL databases | App Services | Storage accounts | All resources | More services

New

Search the Marketplace

Azure Marketplace See all

Popular

Get started

Recently created

Windows Server 2016 Datacenter
Quickstart tutorial

- **Basics:**
- **Subscription**: < select your subscription >
- **Resource group**: az900-rg< the resource group you created earlier >
- **Virtual machine name**: Srv-Work
- **Region**: < The region you selected earlier >
- **Username**: demouser
- **Password**: demo@pass123
- **Public inbound ports**: None

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.
Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? Create VM from Azure Marketplace

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Visual Studio Enterprise – MPN

Resource group * az900-rg
Create new

Instance details

Virtual machine name * Srv-Work

Region * (Asia Pacific) Southeast Asia

Availability options No infrastructure redundancy required

Image * Windows Server 2016 Datacenter
Browse all public and private images

Size * **Standard DS1 v2**
1 vcpu, 3.5 GiB memory
Change size

Administrator account

Username * demouser

Password * ••••••••••••

Confirm password * ••••••••••••

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * None Allow selected ports

Select inbound ports Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Save money

Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

Already have a Windows Server license? * Yes No

Review + create < Previous Next : Disks >

- **Disks:**
- Disk options – OS disk type: Premium SSD

Disk options

OS disk type * Premium SSD

- **Networking:**
- **Virtual Network**: Test-FW-VN
- **Subnet**: Workload-SN
- **Public IP**: None

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	Test-FW-VN Create new
Subnet *	Workload-SN (10.0.2.0/24) Manage subnet configuration
Public IP	None Create new
NIC network security group	○ None ◉ Basic ○ Advanced
Public inbound ports *	◉ None ○ Allow selected ports
Select inbound ports	Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Accelerated networking	○ On ◉ Off

The selected VM size does not support accelerated networking.

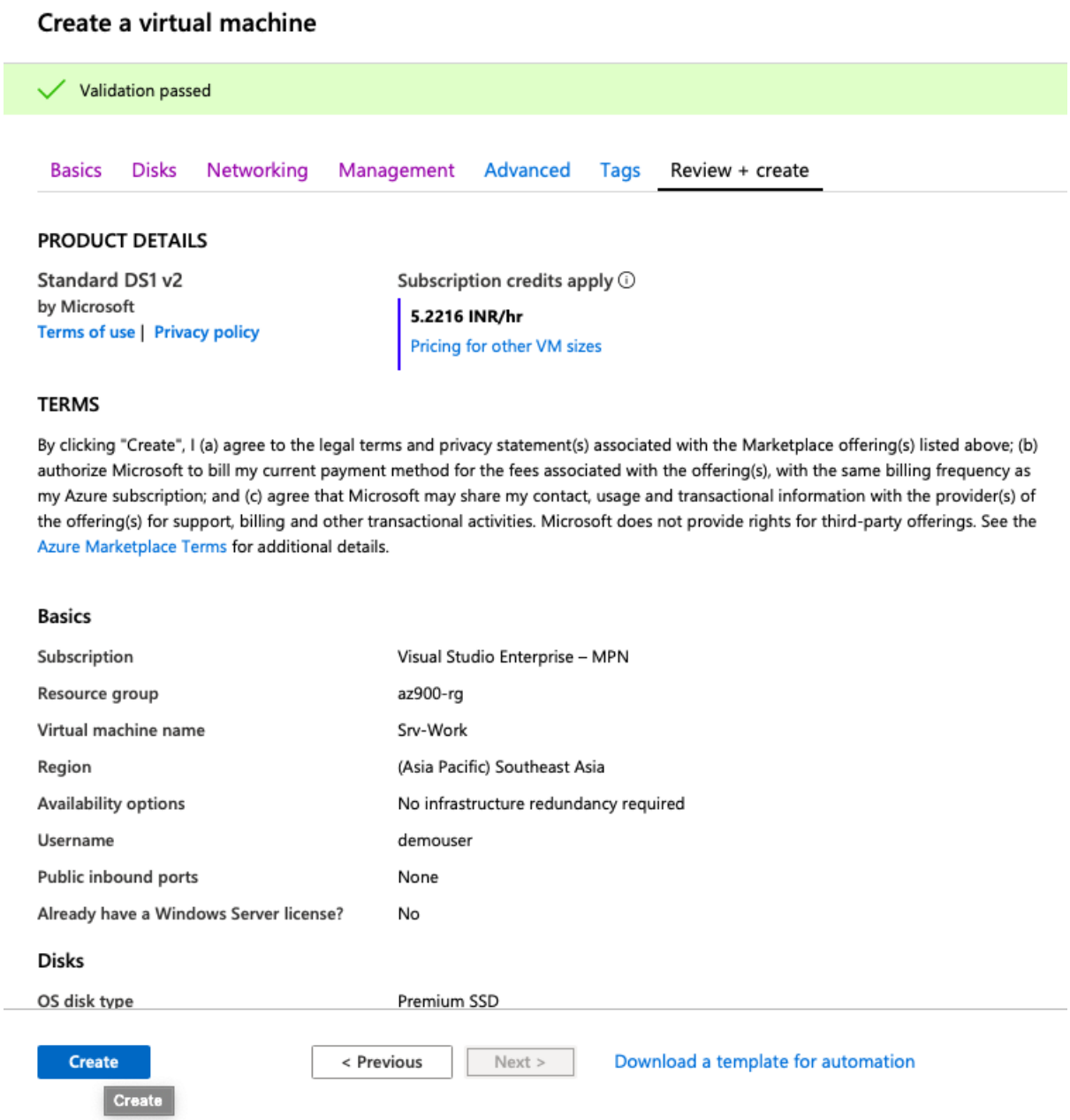
Review + create | < Previous | Next : Management >

- **Management:**
- **Boot diagnostics**: Off

Monitoring

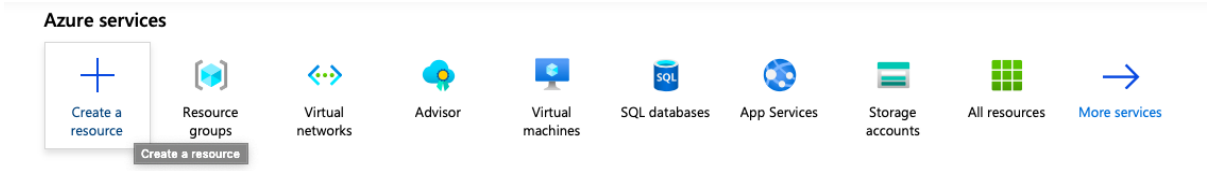
Boot diagnostics	○ On ◉ Off

- Click on create button.

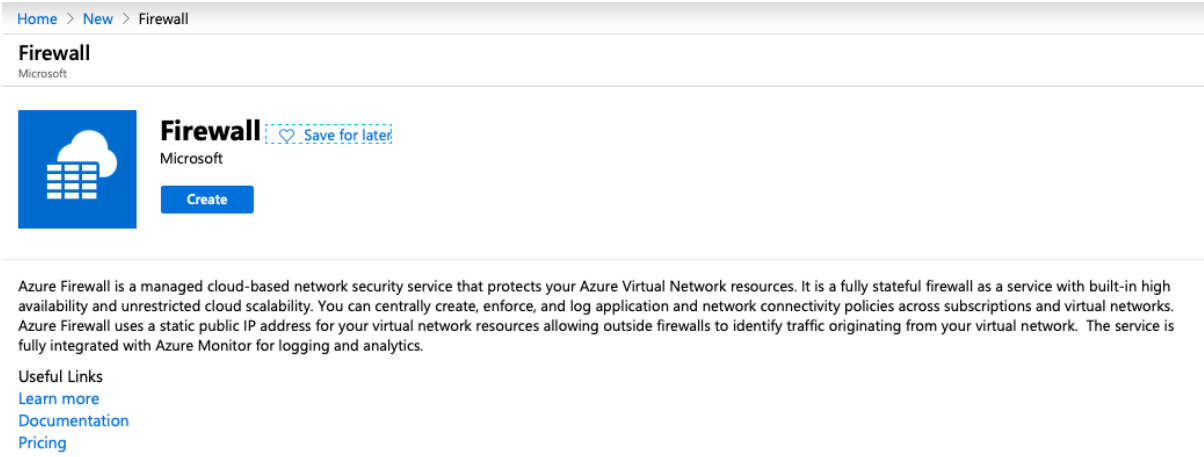


Deploy the Firewall into the VNET

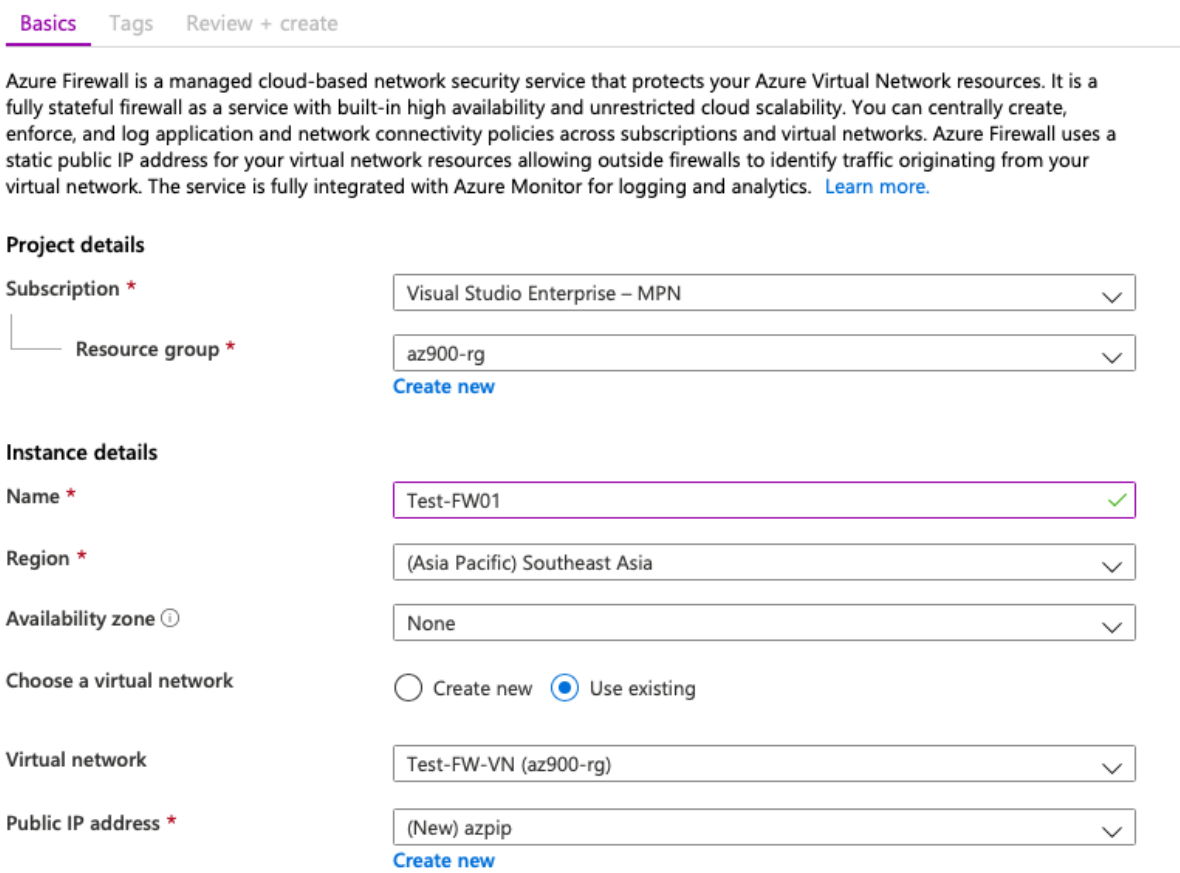
1. From the portal home page, click **Create a resource** and in the **New** pane type **Firewall**, then click **Create**



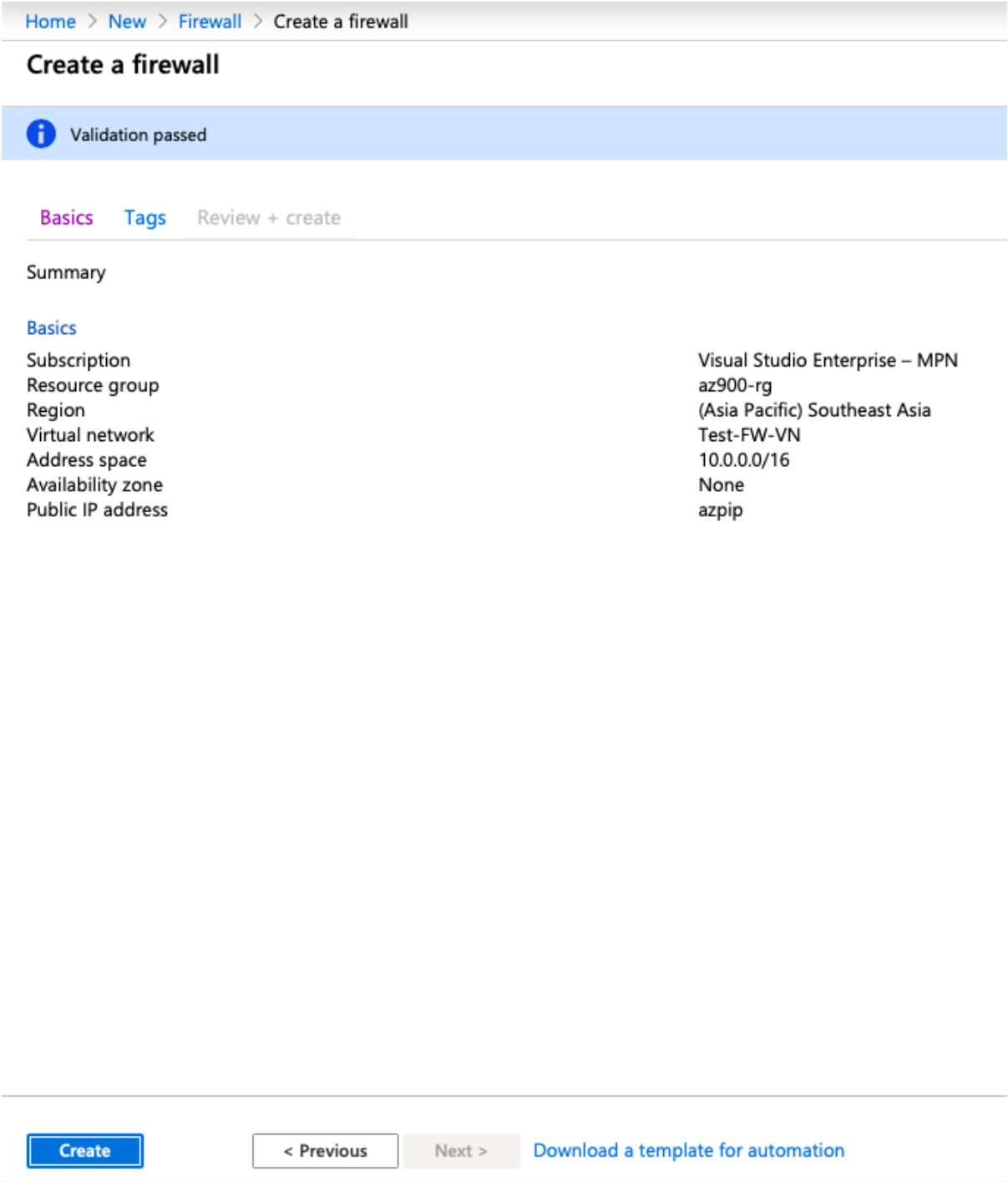
2. Click **Networking** and in the **Featured** section click **See all** > **Firewall** > **Create**.



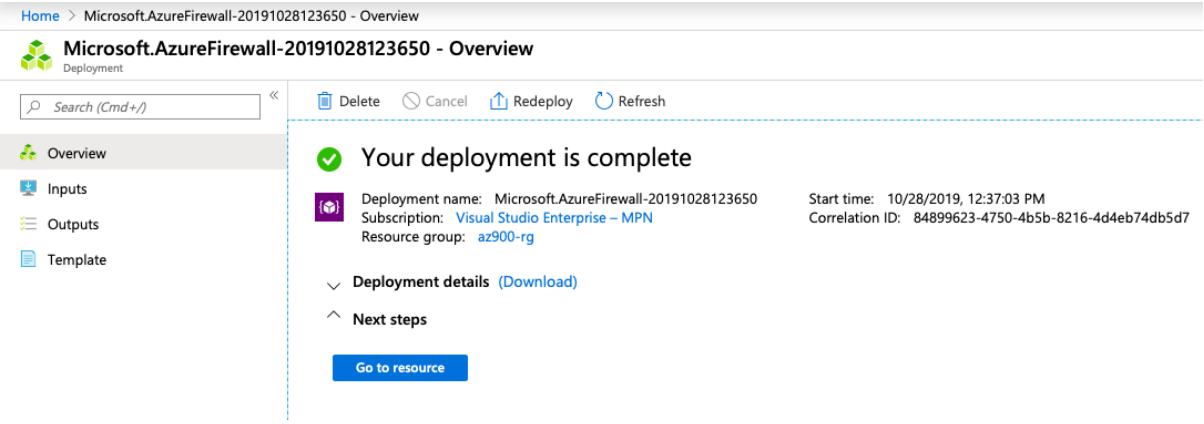
- **Subscription:** < your Azure subscription >
- **Resource group**: az900-rg < the resource group you created earlier >
- **Name**: Test-FW01
- **Region**: < Select the same location that you used previously >
- **Choose a virtual network**: Test-FW-VN < the VNET you created earlier >
- **Public IP address**: < select **Create new** radio button >
- **Public IP address**: < accept the default value >
- **Public IP address SKU**: Standard



Click on create button.

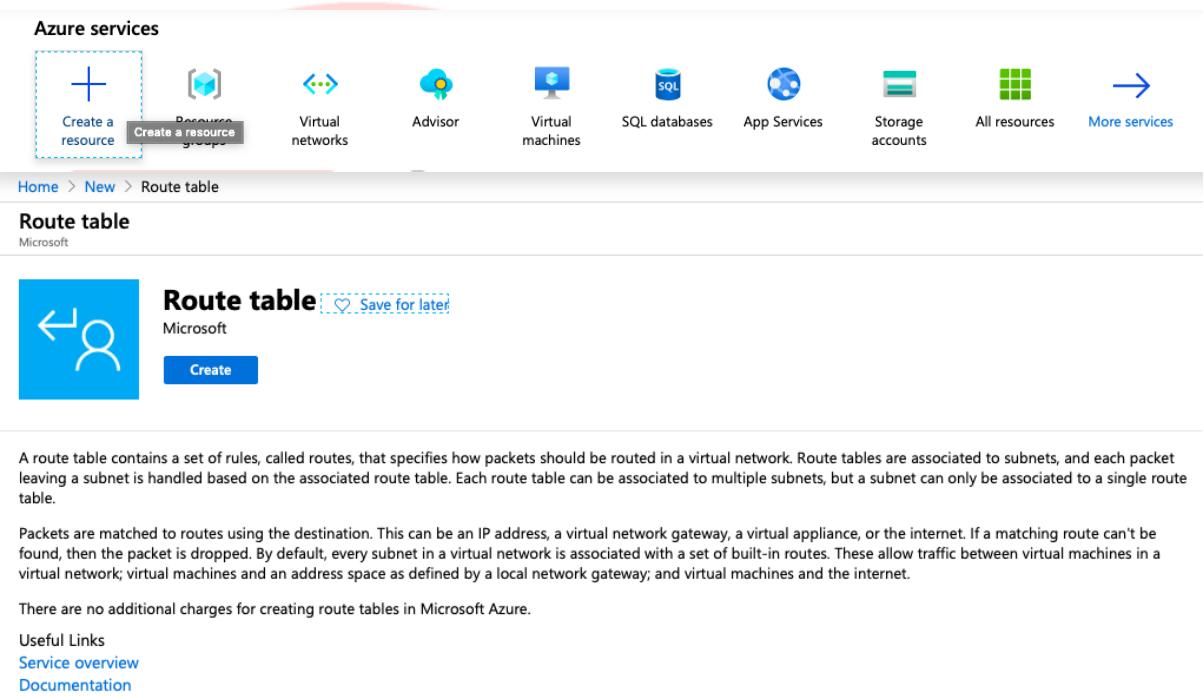


3. After deployment completes, go to the **Test-FW-RG** resource group, and click the **Test-FW01** firewall.

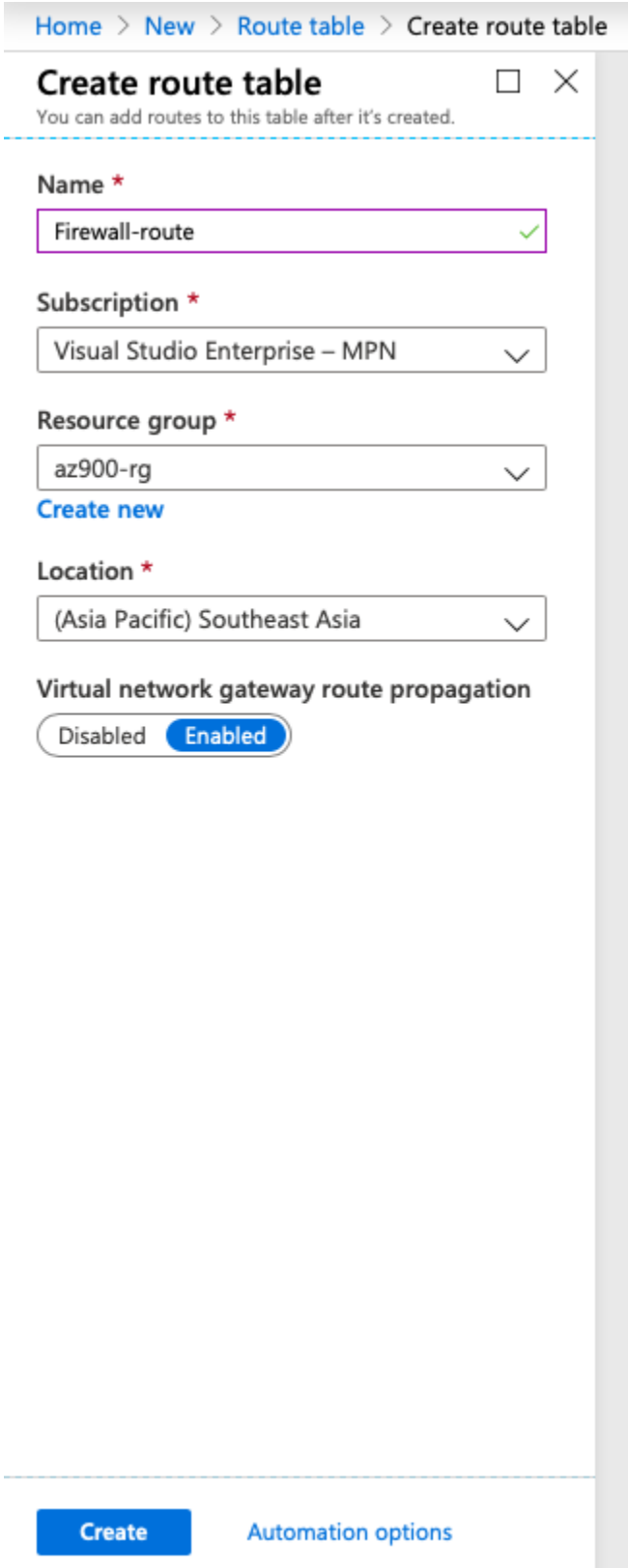


Create a default route

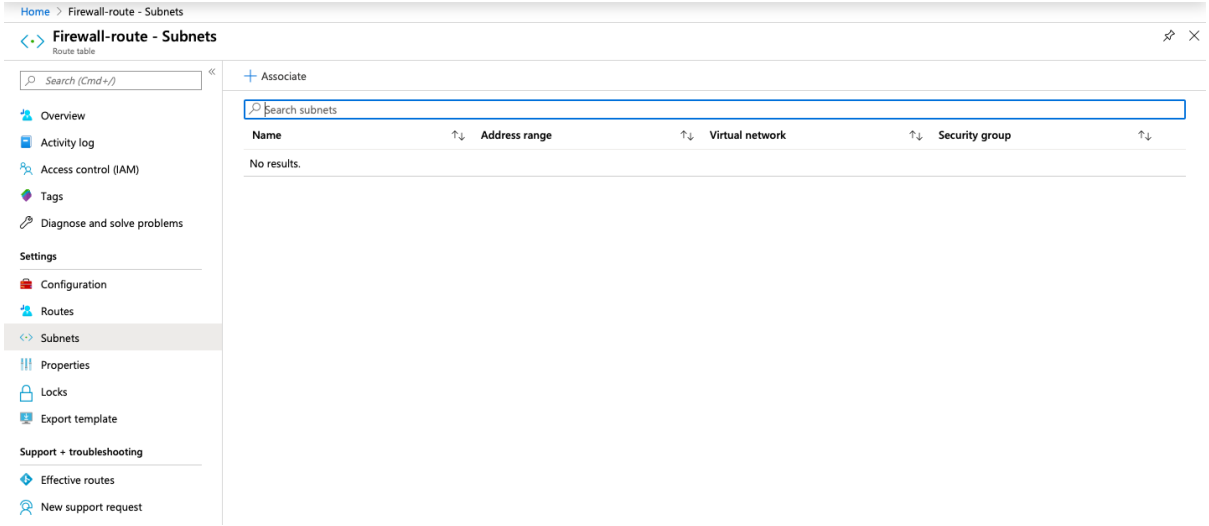
1. From the Azure portal home page, click **All services**. Under **Networking**, click **Route tables**.



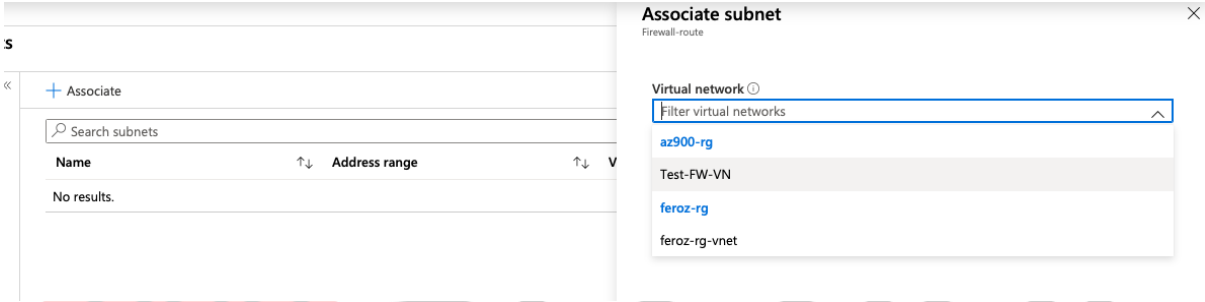
2. In the Route tables pane click **+ Add** and enter the following details and when finished click **Create**
   - **Name**: Firewall-route
   - **Subscription**: < select your subscription >
   - **Resource group**: az900-rg< the resource group you created earlier >
   - **Location**: < select the same location that you used previously >
   - Click on create button.



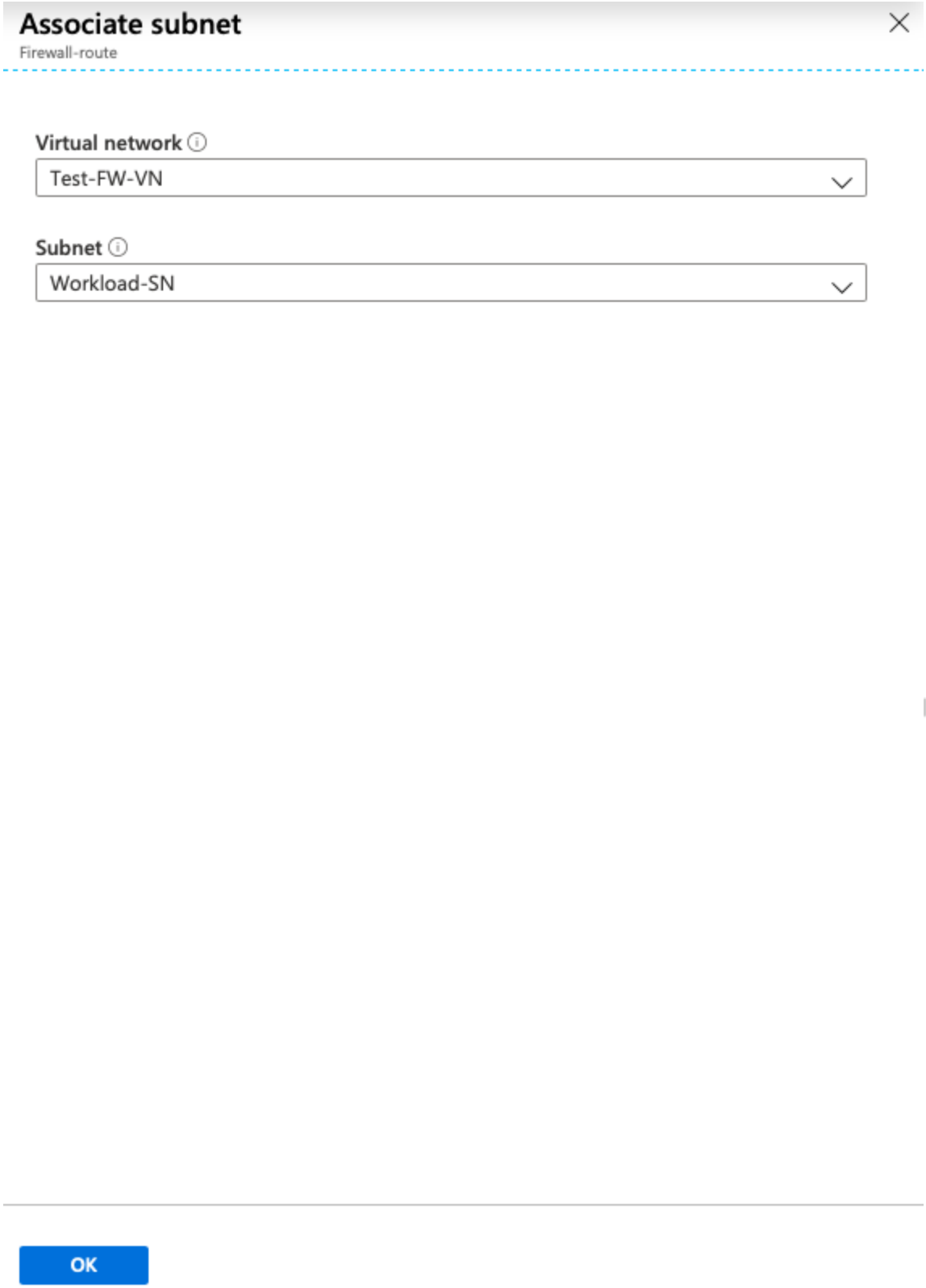
3. When it is finished click **Refresh**, and then click the **Firewall-route** route table.
4. Click **Subnets** > **+ Associate**.



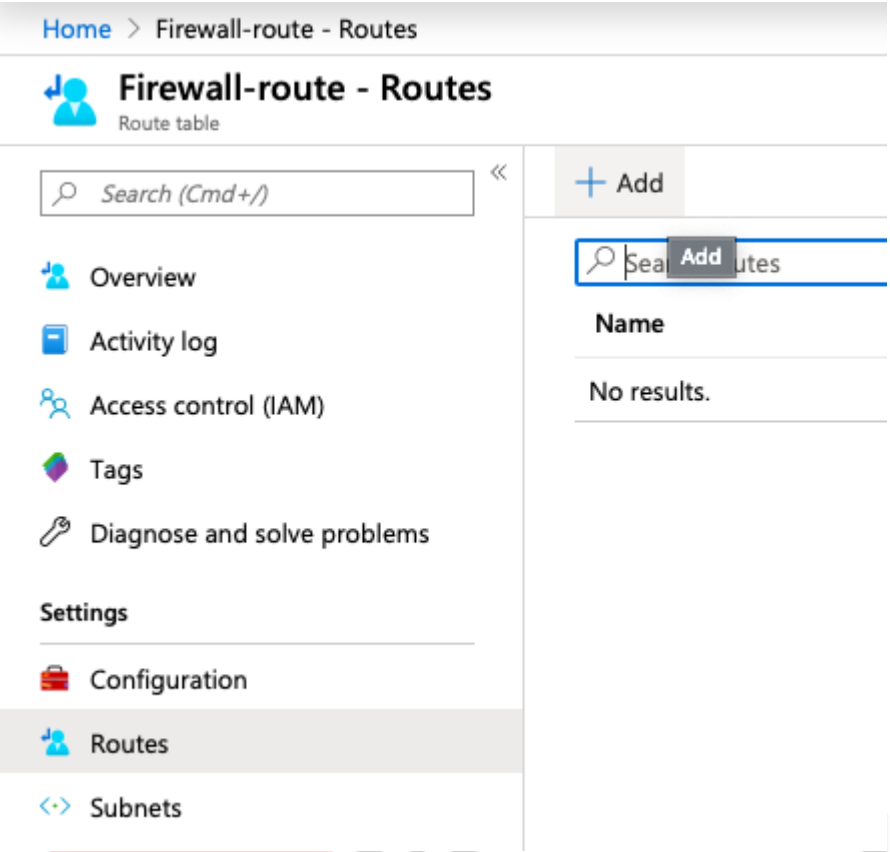
5. Click **Virtual network** > **Test-FW-VN**.



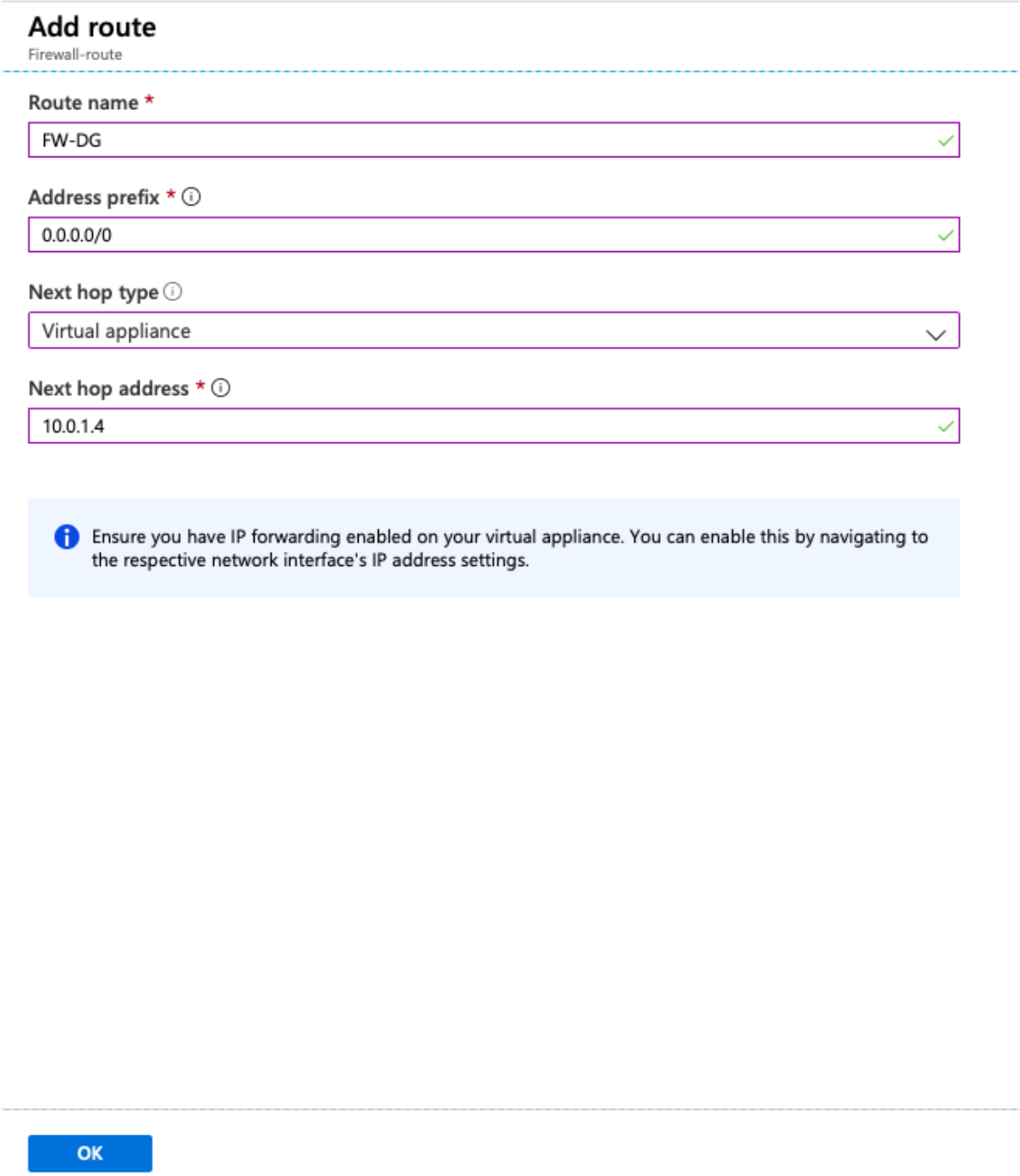
6. For **Subnet**, click **Workload-SN**. Make sure that you select **only** the **Workload-SN** subnet for this route, otherwise your firewall won't work correctly.
7. Click OK.



8. Click **Routes** > **+ Add** and enter the following details and click **OK** when finished

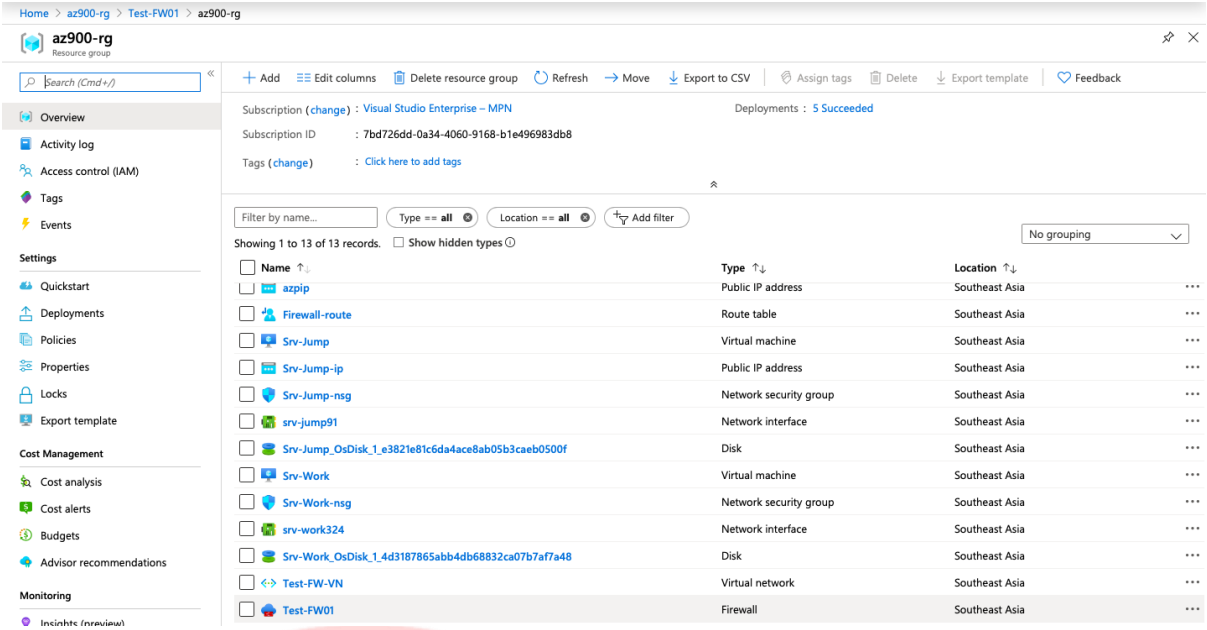


- **Route name**: FW-DG
- **Address prefix**: 0.0.0.0/0
- **Next hop type**: Virtual appliance. (Azure Firewall is actually a managed service, but *virtual appliance* works in this situation.)
- **Next hop address** < enter the private IP address for the firewall that you noted previously >

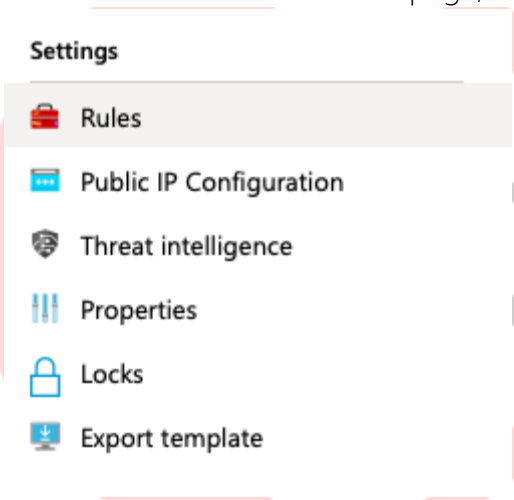


Configure an application rule

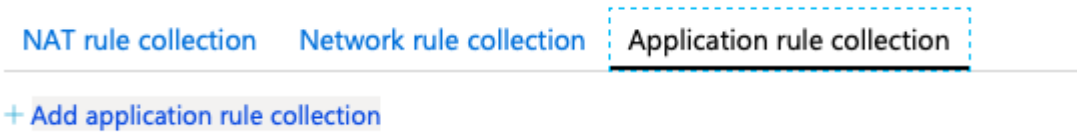
1. Open the **az900-rg**, and click the **Test-FW01** firewall.\



2. On the Test-FW01 page, under Settings, click Rules.



3. Click the **Application rule collection** tab.



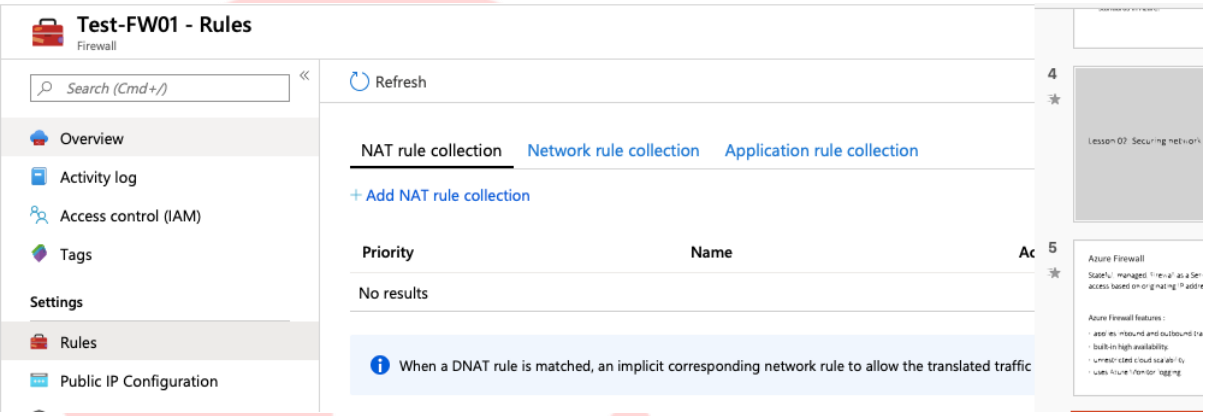
4. Click **+ Add application rule collection** and enter the following values, then click **Add** when finished
    - **Name**: App-Coll01
    - **Priority**: 200
    - **Action**: Allow
    - **Rules:**
    - **Name:** AllowWebsite
    - **Source Address**:10.0.2.0/24.
    - **Protocol:Port**: http, https.

- **Target FQDNS:** www.microsoft.com (You can specify part of all or a URL, including wild characters, or just a single wild character to indicate all internet sites)

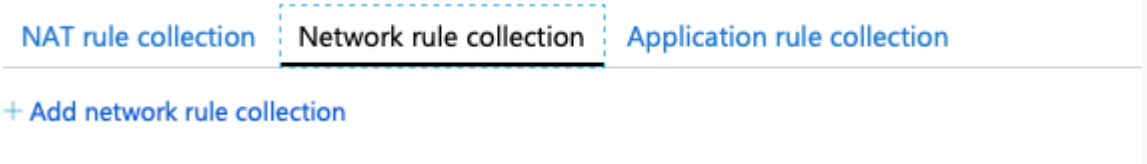
Note: Azure Firewall includes a built-in rule collection for infrastructure FQDNs that are allowed by default. These FQDNs are specific for the platform and can't be used for other purposes. For more information, see Infrastructure FQDNs. You can also use FQDN tags to represent a group of fully qualified domain names (FQDNs) associated with well known Microsoft services, such as Windows Update, Azure Backup etc.

Configure a network rule:

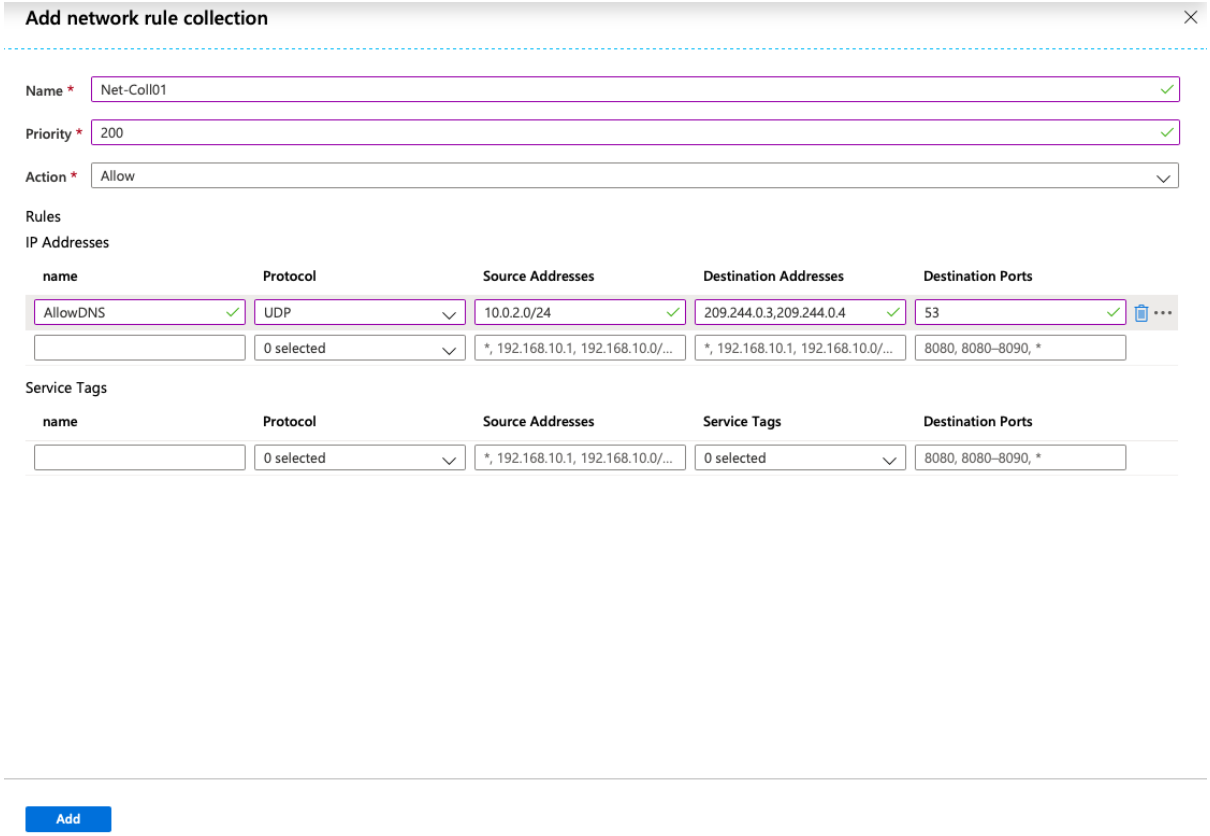
1. Open the **az900-rg**, and click the **Test-FW01** firewall.
2. On the **Test-FW01** page, under **Settings**, click **Rules**>Click the **Network rule collection** tab.



3. Click **+ Add network rule collection** and enter the following details, when finished click **Add**

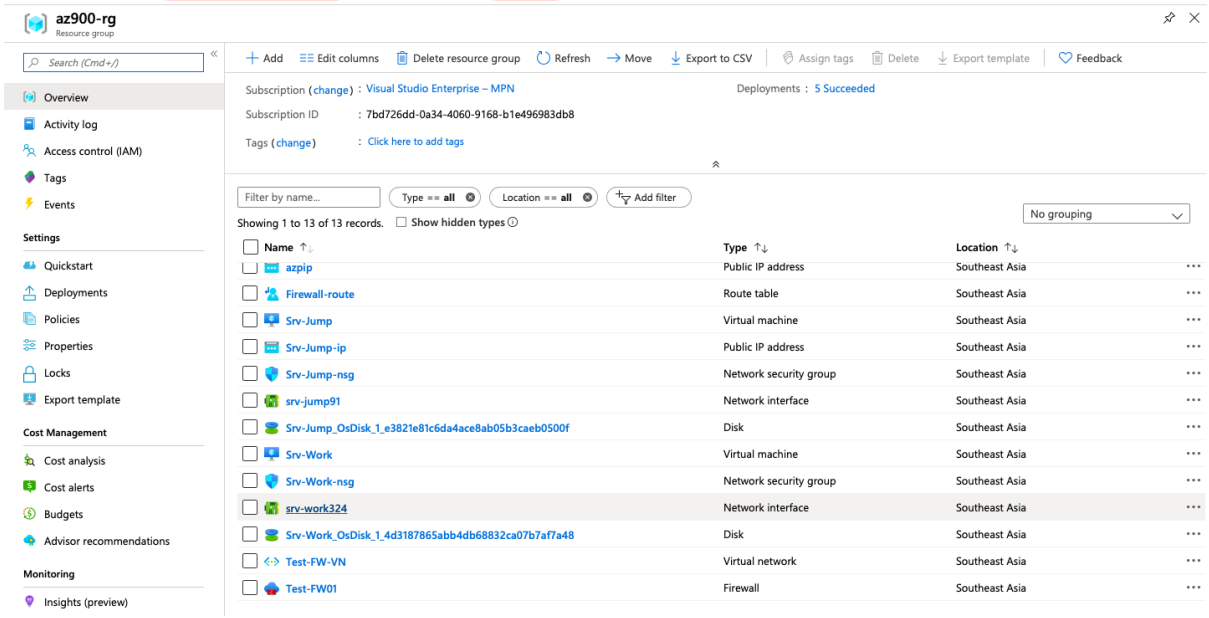


- **Name**: Net-Coll01
- **Priority**: 200
- **Action**: Allow
- **Rules:**
- **IP Addresses**:
- **Name:** AllowDNS
- **Protocol**: UDP
- **Source Addresses**: 10.0.2.0/24
- **Destination Addresses:** 209.244.0.3,209.244.0.4
- **Destination Port:**: 53

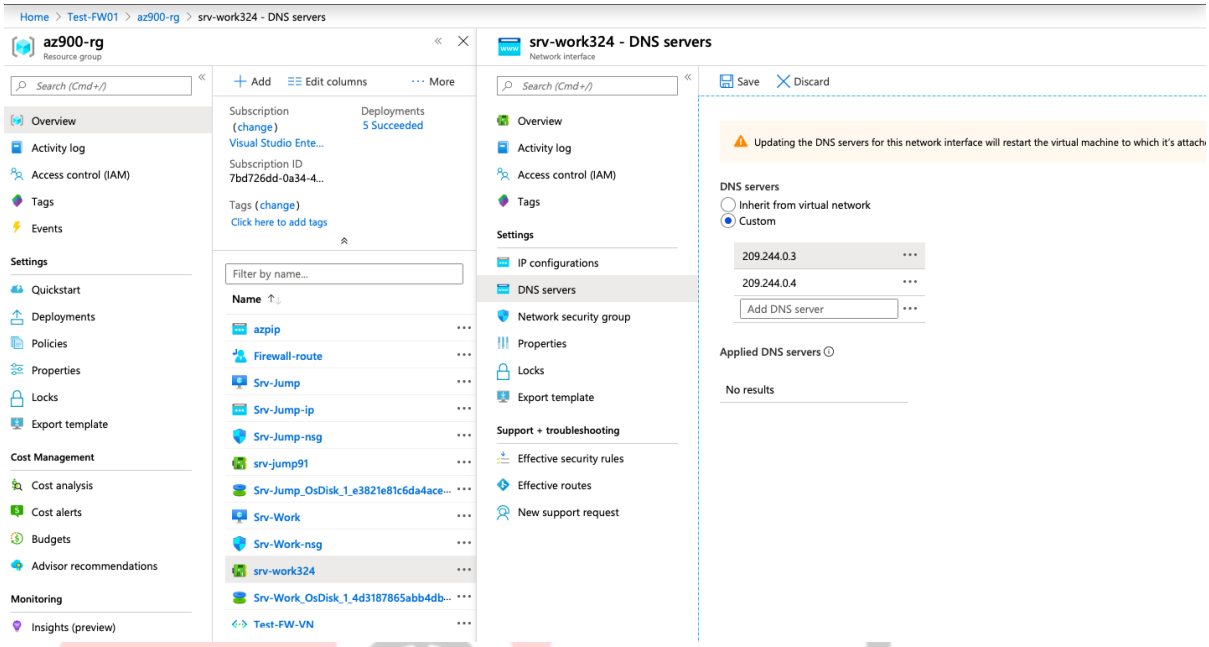


Change the primary and secondary DNS address for the Srv-Work network interface

1. From the Azure portal, open the **az900-rg** resource group.
2. Click the **network interface** for the **Srv-Work** virtual machine, it should be named something like *Srv-Work-xyz*.

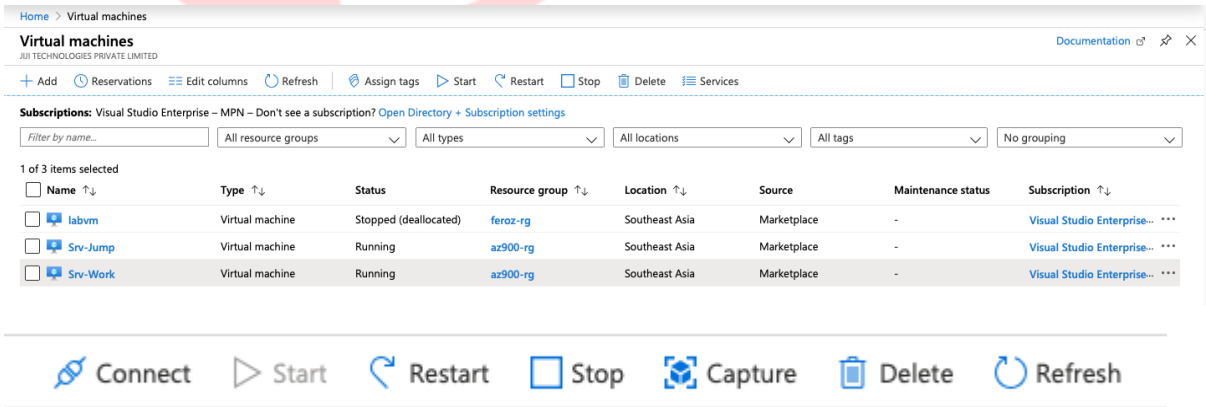


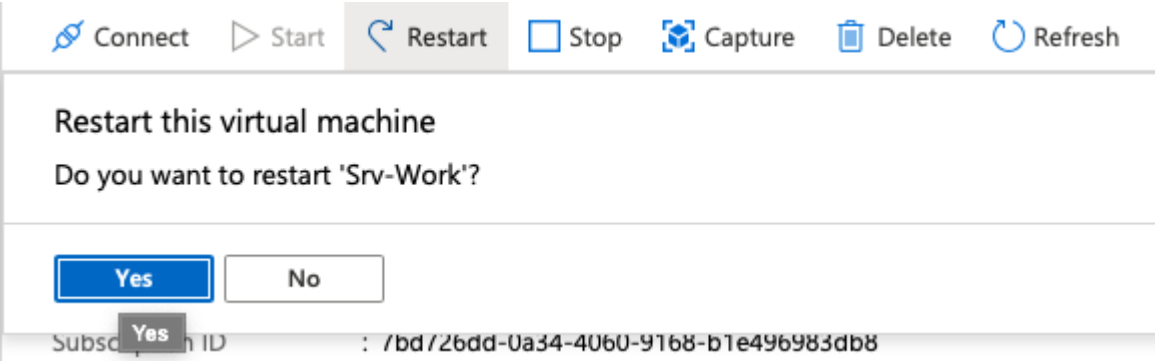
3. Under **Settings**, click **DNS servers**.> click **Custom** and add the following details and click **Save** when finished.
   - **Box 1 - Add DNS Server**: 209.244.0.3
   - **Box 2 - Add DNS Server**: 209.244.0.4



Note: Updating the DNS records for the Network interface will automatically restart the virtual machine to which it is attached, you should see a message indicating such. Also the IP Addresses we are adding here are pre-existing publicly accessible DNS Server addresses. When our virtual machine looks for an external address it will refer to these DNS servers for the address details.

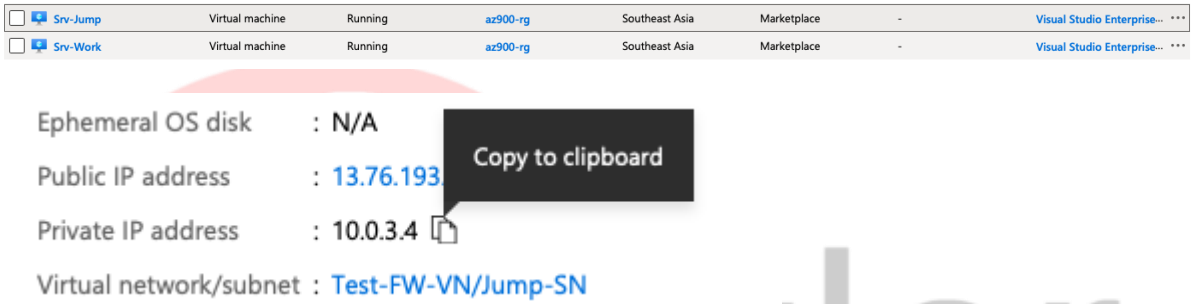
4. Go to the Srv-Work virtual machine and ensure it has a status of running, if it is de-allocated click **Start**, or if it has not re-started click **Restart**



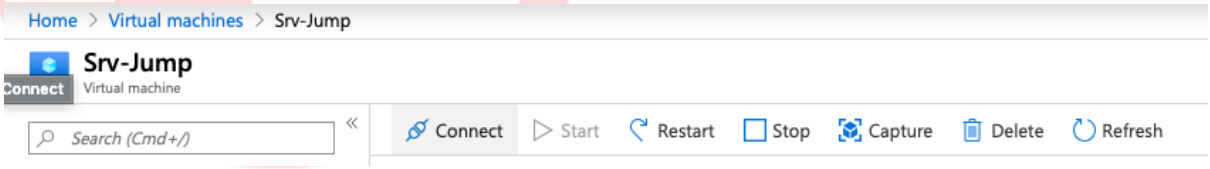


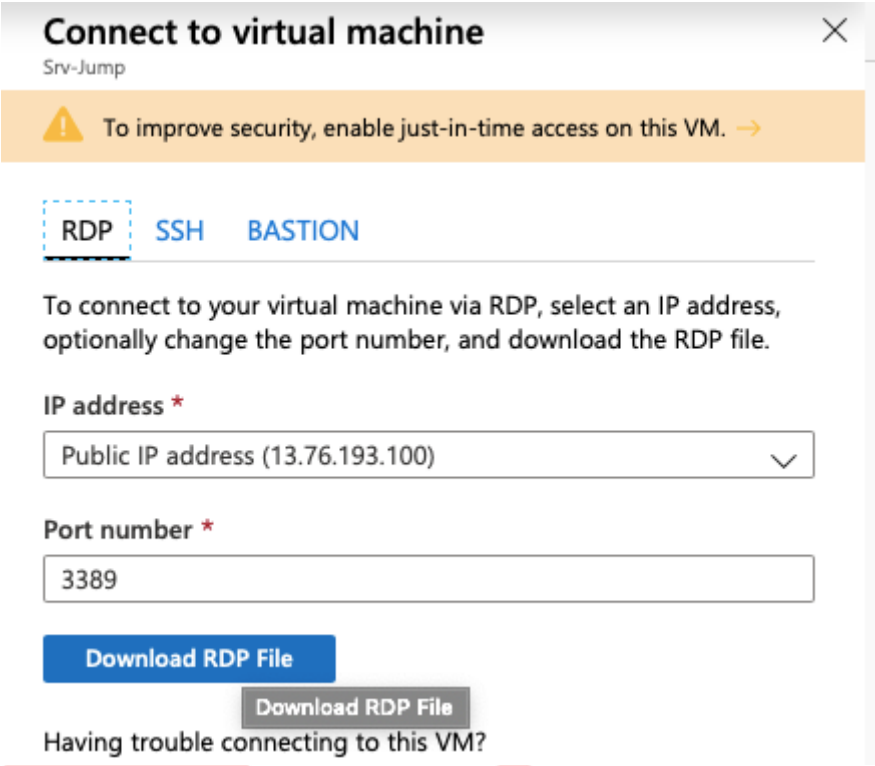
Test the firewall

1. From the Azure portal, review the network settings for the **Srv-Work** virtual machine and note the private IP address.

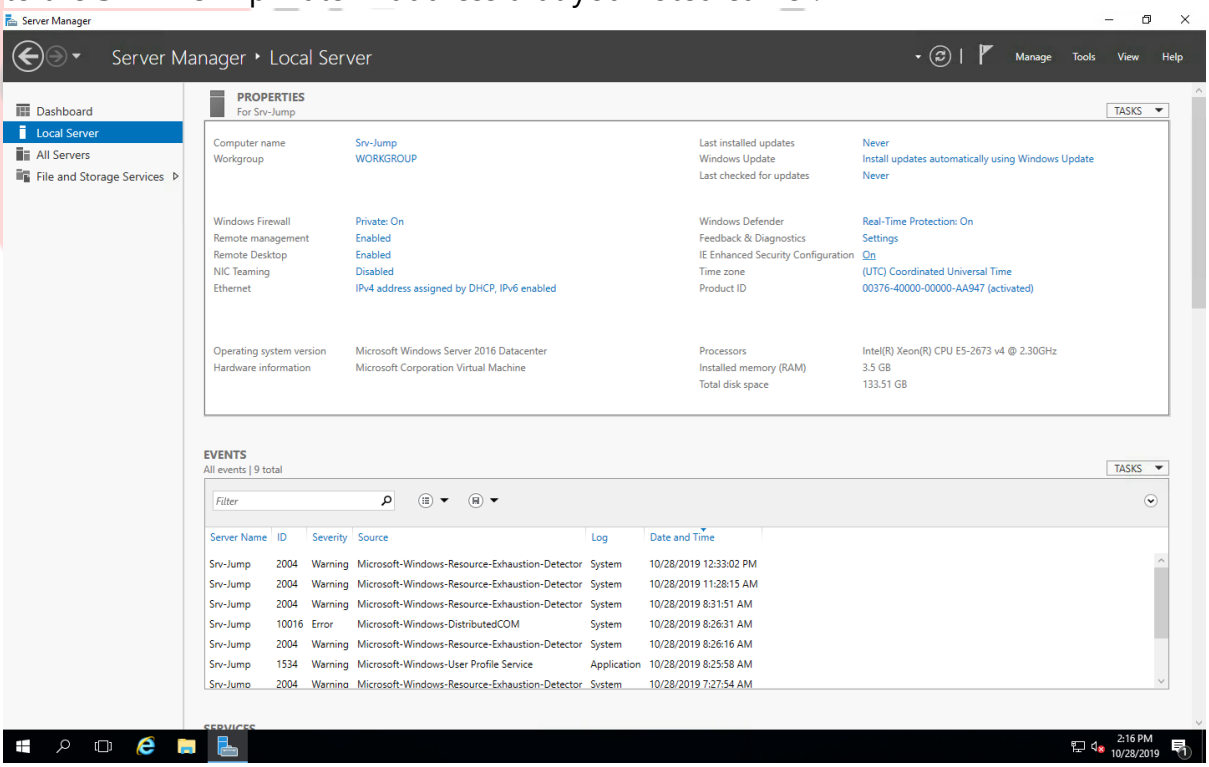


2. In the Azure Portal go to the **Srv-Jump** virtual machine and click **Connect**, followed by **Download RDP File** to open an RDP session to the **SRV-Jump** virtual machine, using the credentials you specified earlier when creating the VM.





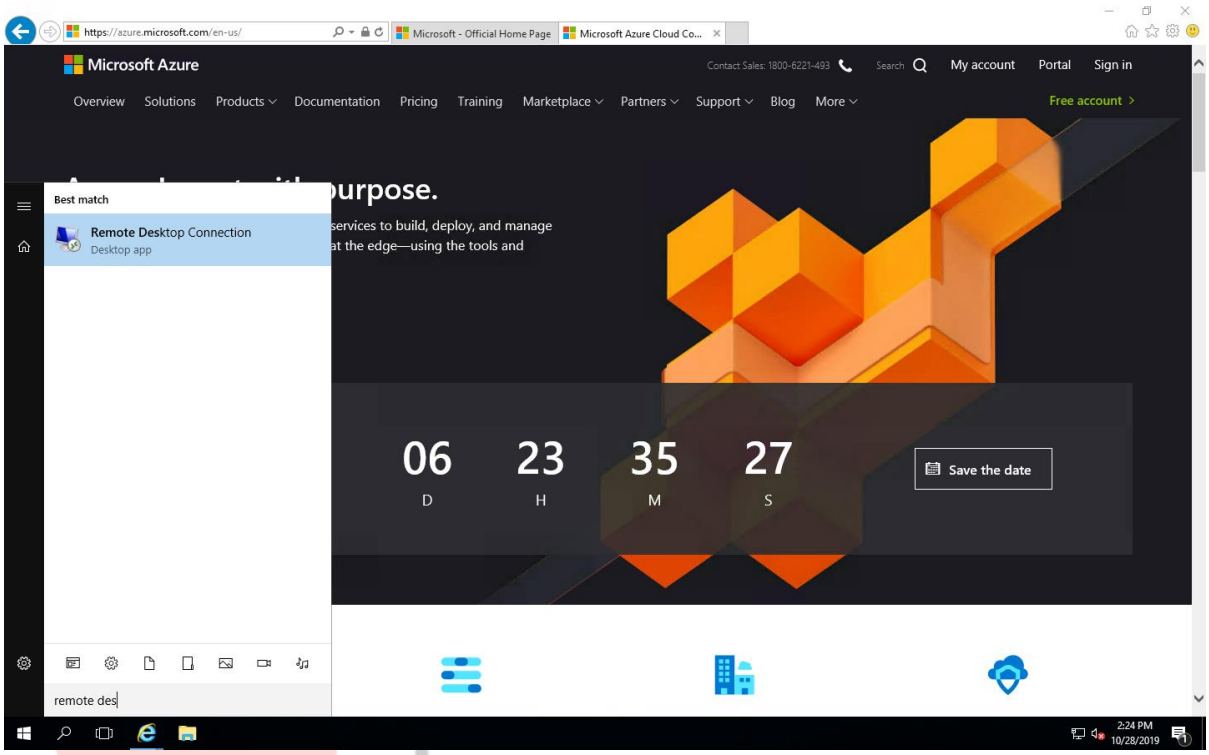
3. From within the **Srv-Jump** virtual machine open a remote desktop connection to the **Srv-Work** private IP address that you noted earlier.



4. Once logged into the SRV-Jump virtual machine, allow **Server Manager** to open, which it will do after log in automatically, then go to **Local server** and turn off **IE Enhanced Security Configuration.**

Note: In production environments you would not do this, this is to allow use access the workload server a bit more easily in this test scenario and reduce and prevent pop-ups. In a production you may use a workload server with no GUI environment present.

5. Open **Internet Explorer** and browse to https://www.microsoft.com



6. Click **OK** > **Close** on the security alerts that may pop-up.