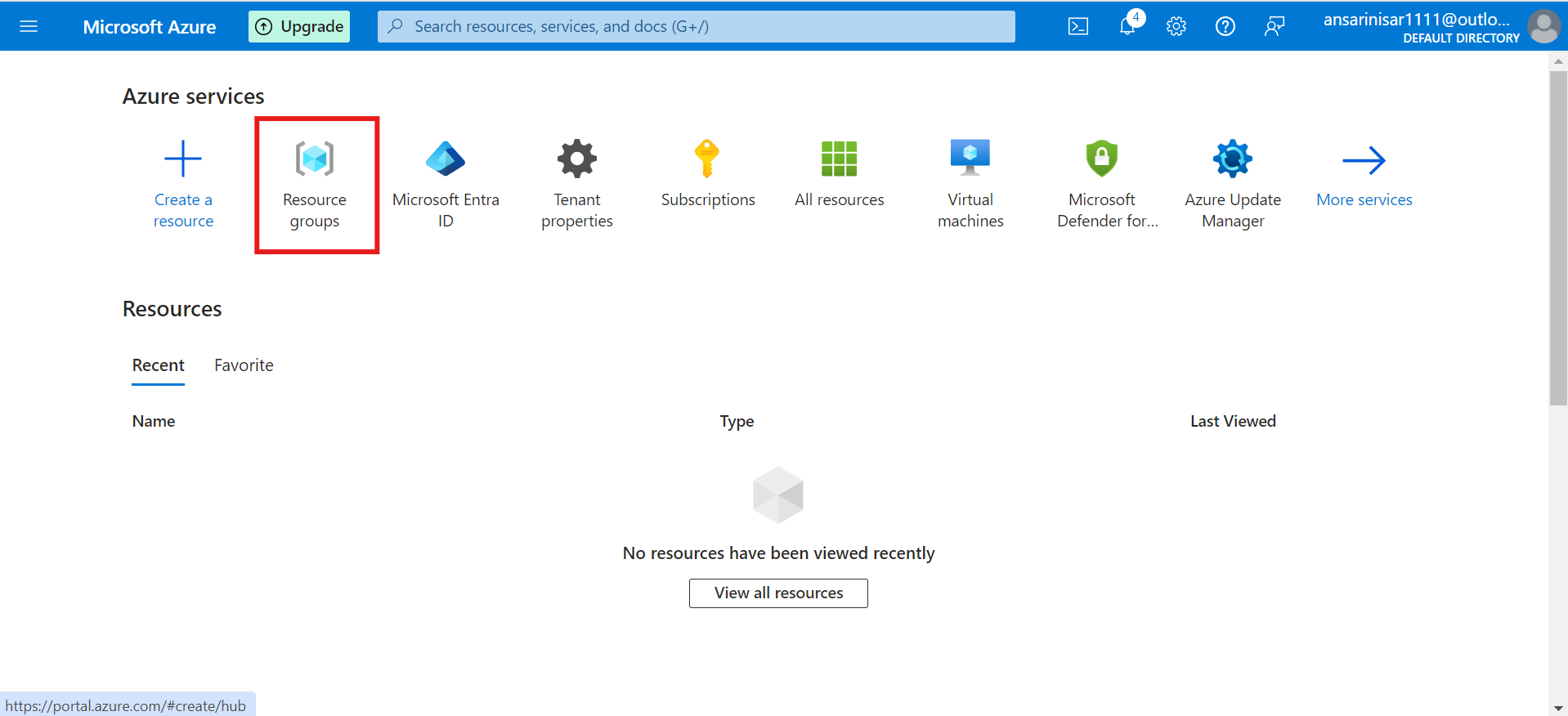
**Azure Firewall**

A firewall is a security system designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet. By analyzing data packets, firewalls can block or permit traffic based on criteria like IP addresses, domain names, protocols, and ports. There are different types of firewalls, including hardware-based, software-based, or a combination of both, each offering varying levels of protection. Firewalls are crucial in defending against unauthorized access, cyberattacks, and various threats by filtering traffic and preventing potentially harmful data from entering or leaving a network.

Azure Firewall is a cloud-native, stateful firewall service provided by Microsoft Azure, designed to offer comprehensive network security for Azure Virtual Networks. It enables users to define and enforce security policies to control both inbound and outbound traffic, ensuring robust protection against cyber threats. Azure Firewall integrates seamlessly with other Azure services, providing advanced features like threat intelligence-based filtering, high availability, and scalability. It supports both application and network-level filtering, allowing for detailed traffic inspection and policy enforcement. With built-in monitoring and logging capabilities, Azure Firewall helps organizations maintain visibility into their network traffic and adapt to evolving security needs, all while leveraging the flexibility and power of Azure's cloud infrastructure.

**Steps to Creating, Deploying and Configuring the Firewall: -**

Step 1- Go to the Azure dashboard and select the Resource Group option in order to create a resource group.



Step 2- Now click on the create button.

A screenshot of a computer

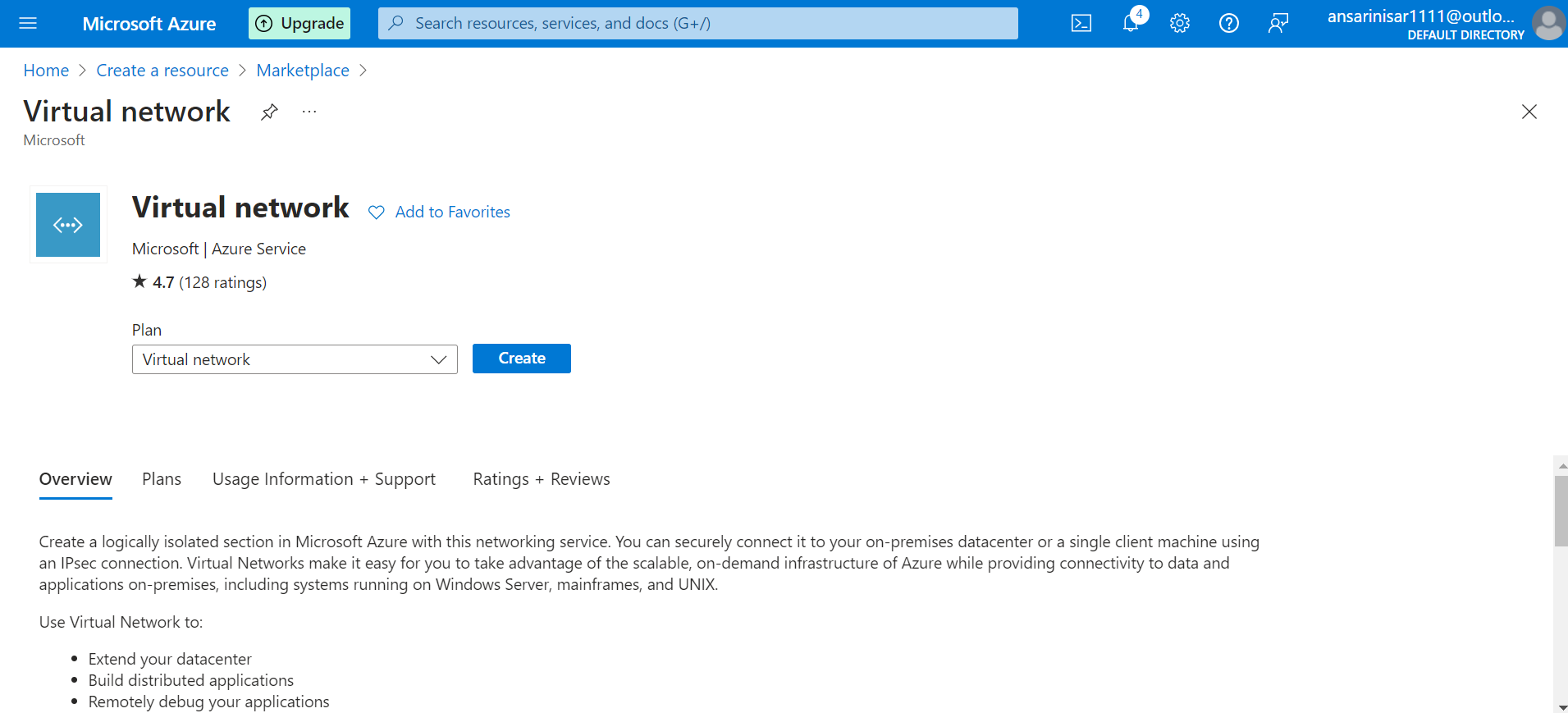
Description automatically generated

Step 3- Now fill up the basic details related to the RG.

A screenshot of a computer

Description automatically generated

Step 4- Now we are going to create a virtual network. To do so, go to the virtual network tab.



Step 5- Now provide the basic details related to the virtual network.

A screenshot of a computer

Description automatically generated

Step 6- Now we have to create a IP address with a range for our virtual network.

A screenshot of a computer

Description automatically generated

Step 7- Now we have to add a subnet to our V-net. To do the same, click on the add subnet button and define some basic details related to it.

A screenshot of a computer

Description automatically generated

Step 8- After giving all the details just review once and click on the create button.

A screenshot of a computer

Description automatically generated

Step 9- Now we have to peer our V-net to another V-net. To do same, click on the peerings option.

A screenshot of a computer

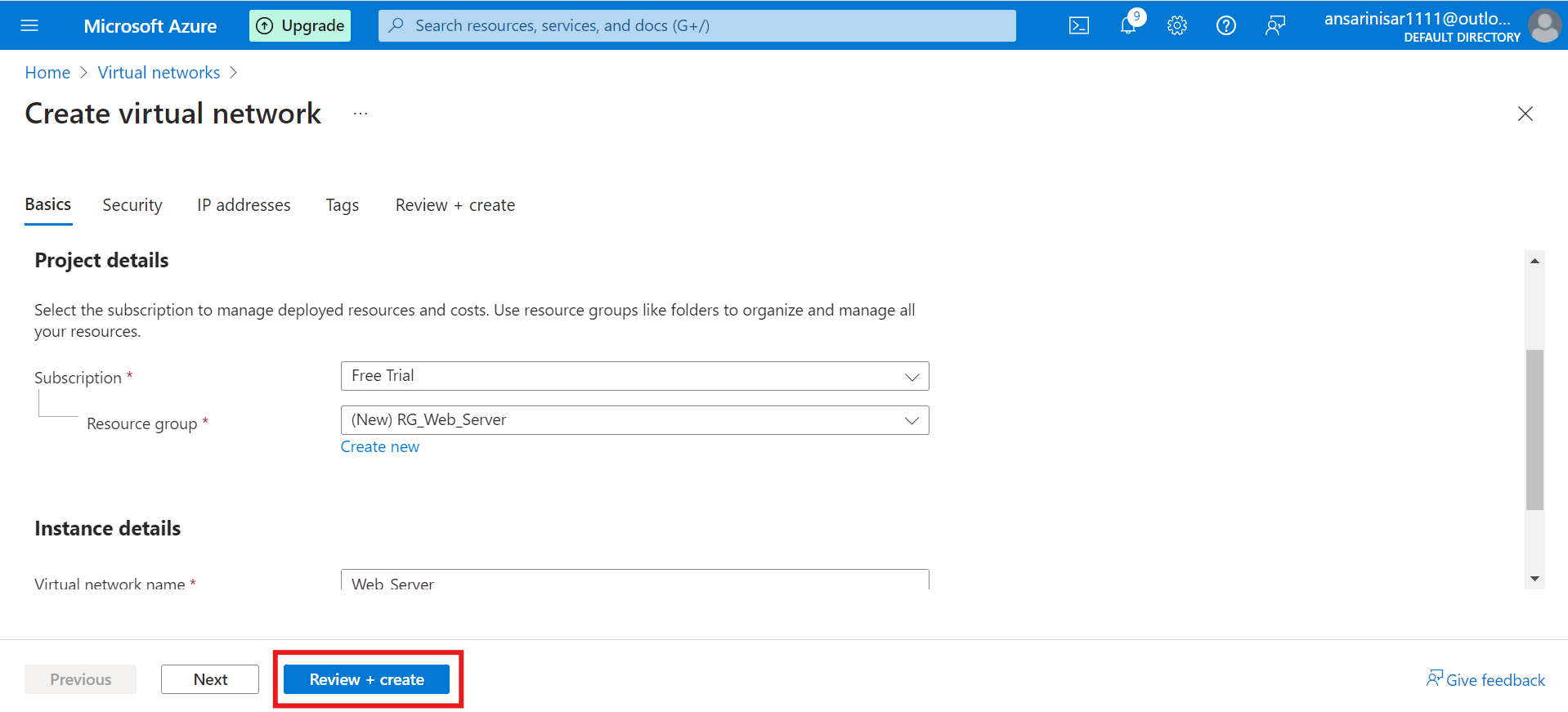
Description automatically generated

Step 10- Now to create a peer click on the add button.

A screenshot of a computer

Description automatically generated

Step 11- Now pass the basic details about the peering and click on the create button.



Step 12- Now just create a virtual network and click on the create button.

A screenshot of a computer

Description automatically generated

Step 13- Next we have to define the peering name and virtual network.tual network.

A screenshot of a computer

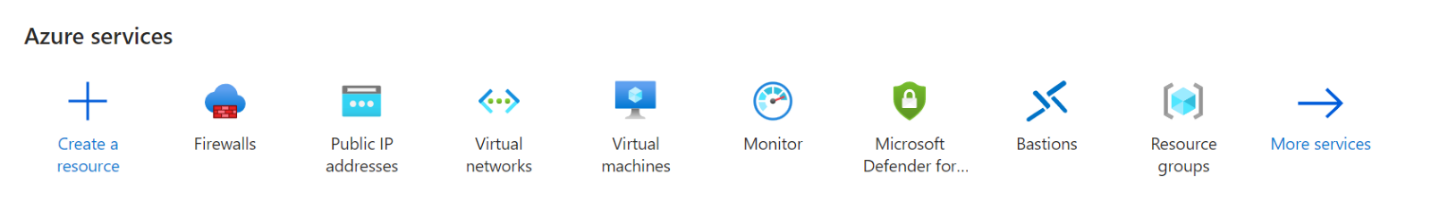
Description automatically generated

Step 14- After that click on the create button.

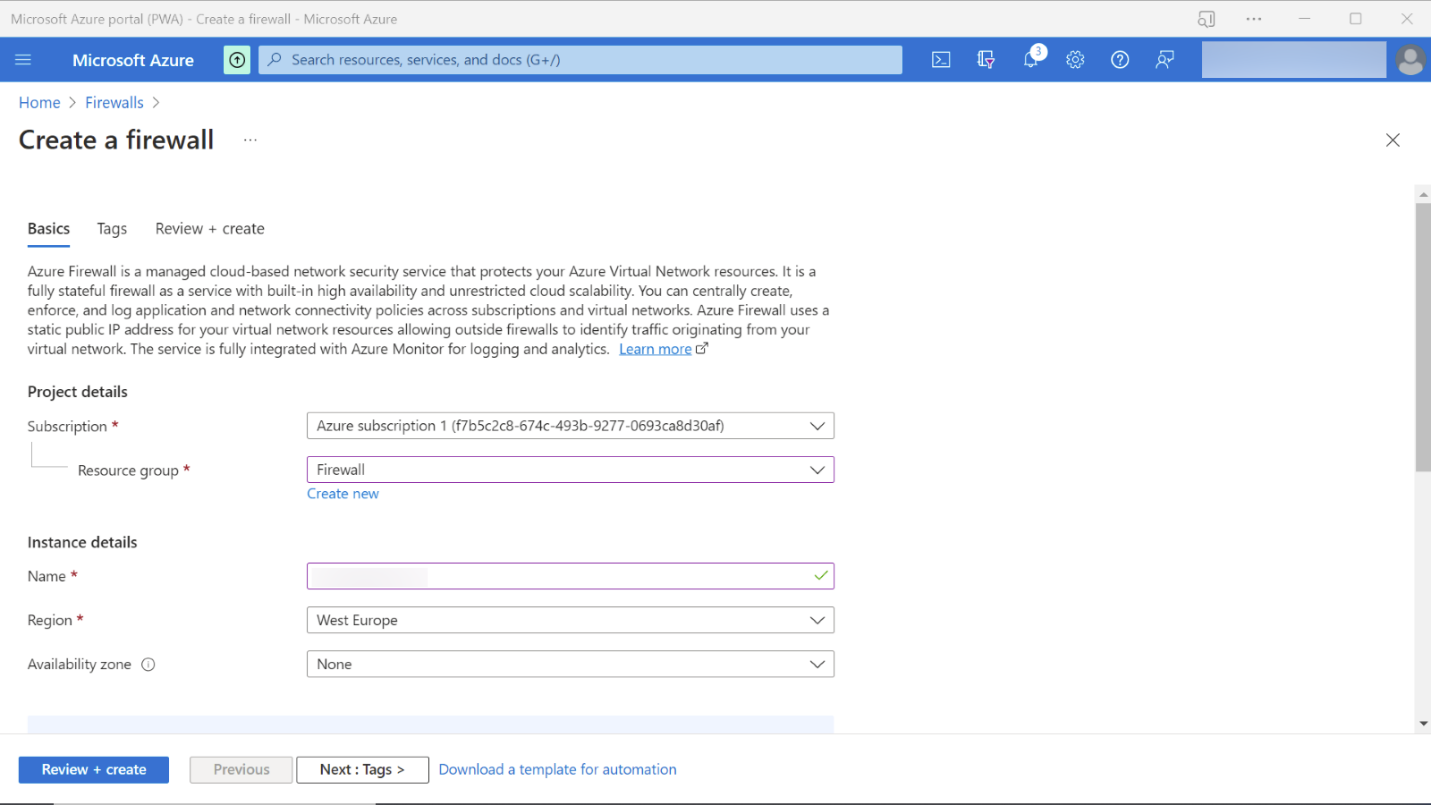
A screenshot of a computer

Description automatically generated

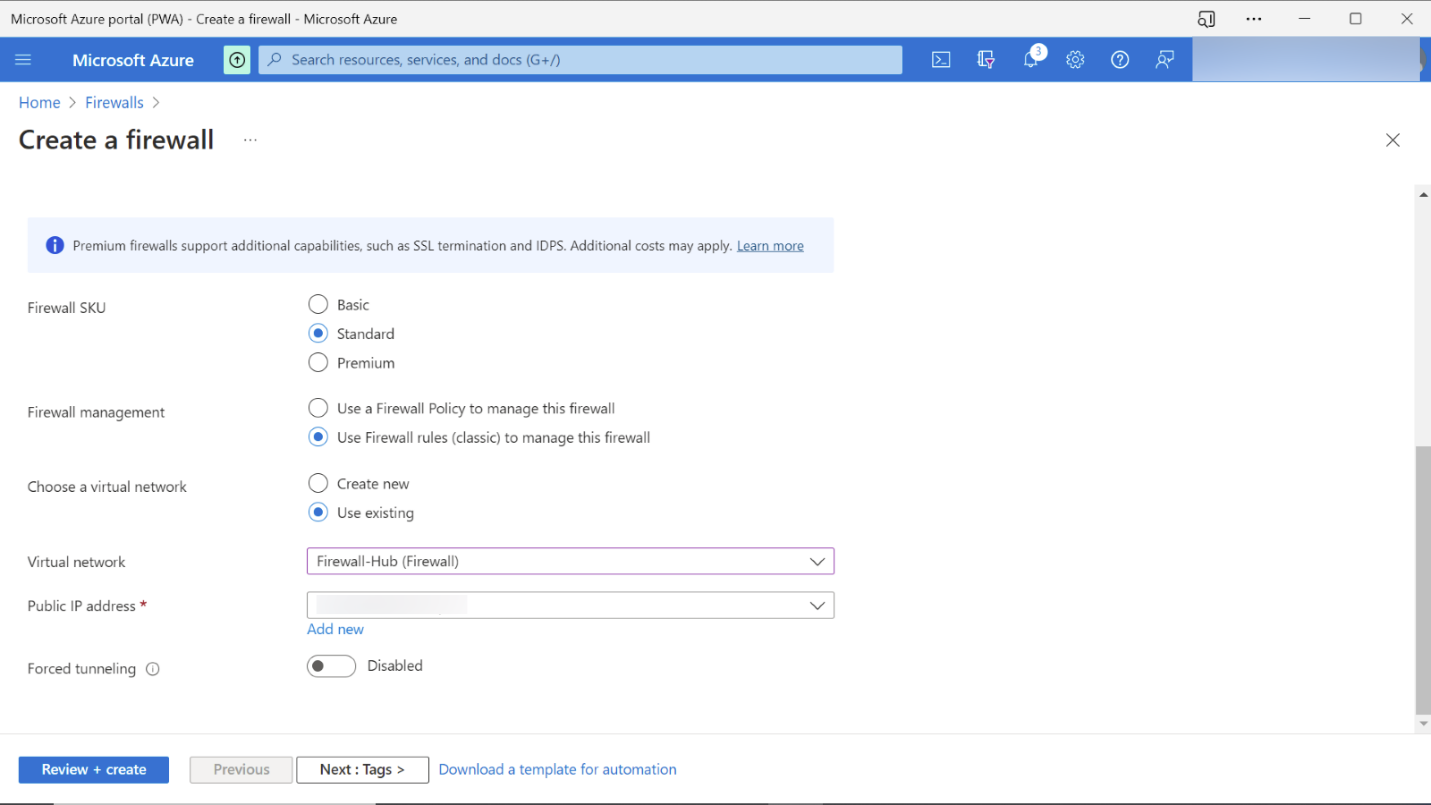
Step 15- Now to create a Firewall choice the Firewall option from the dashboard.



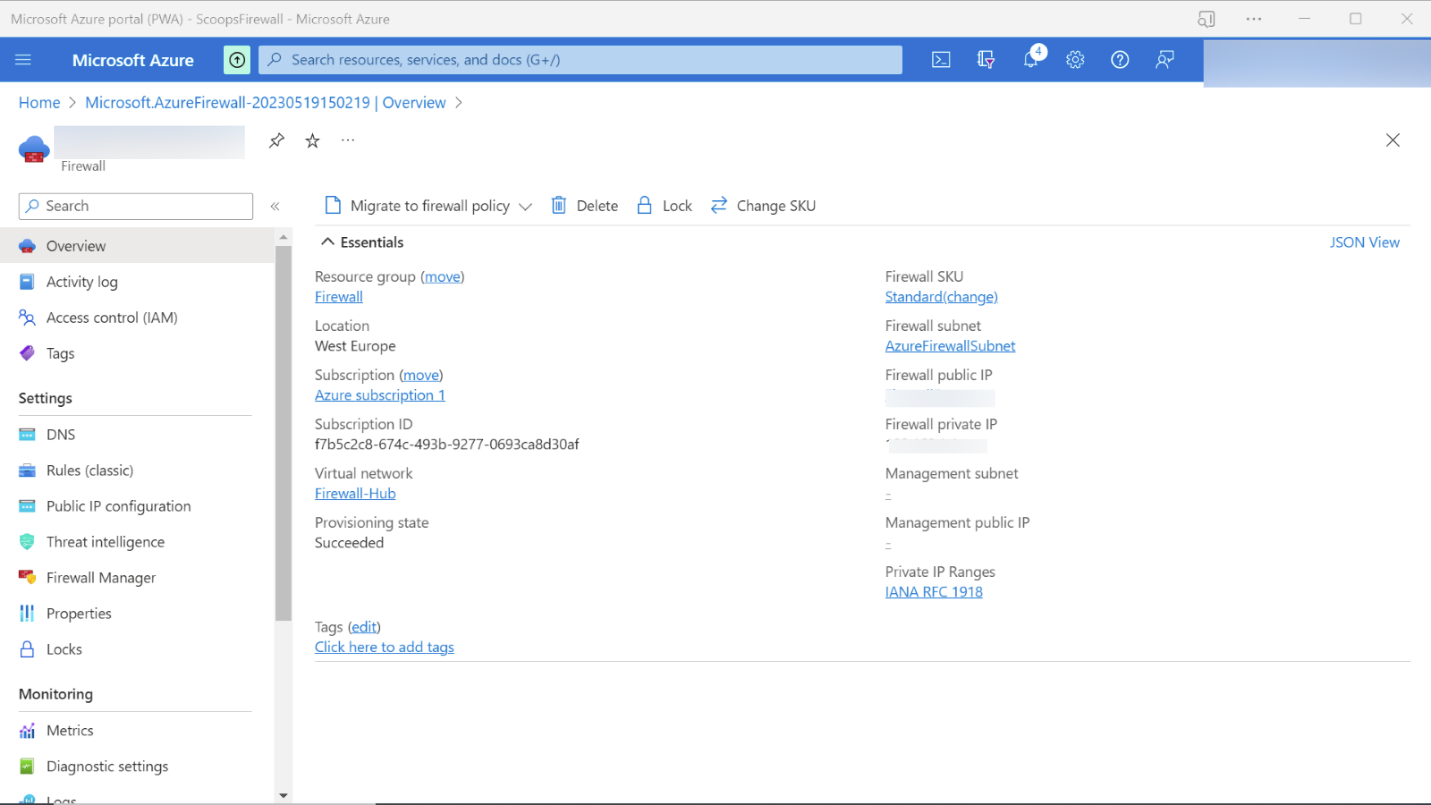
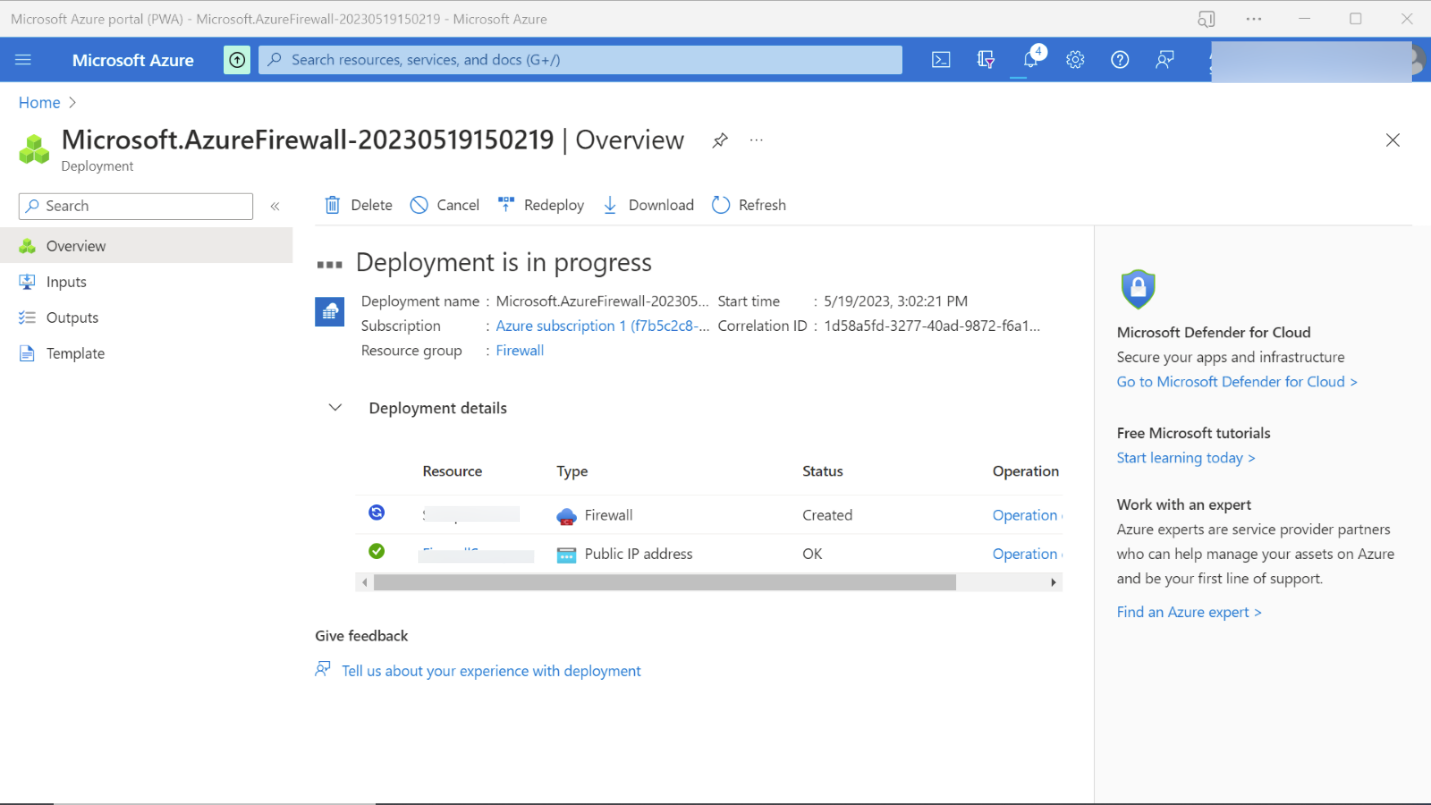
Step 16- Now provide basic information related to the Firewall.



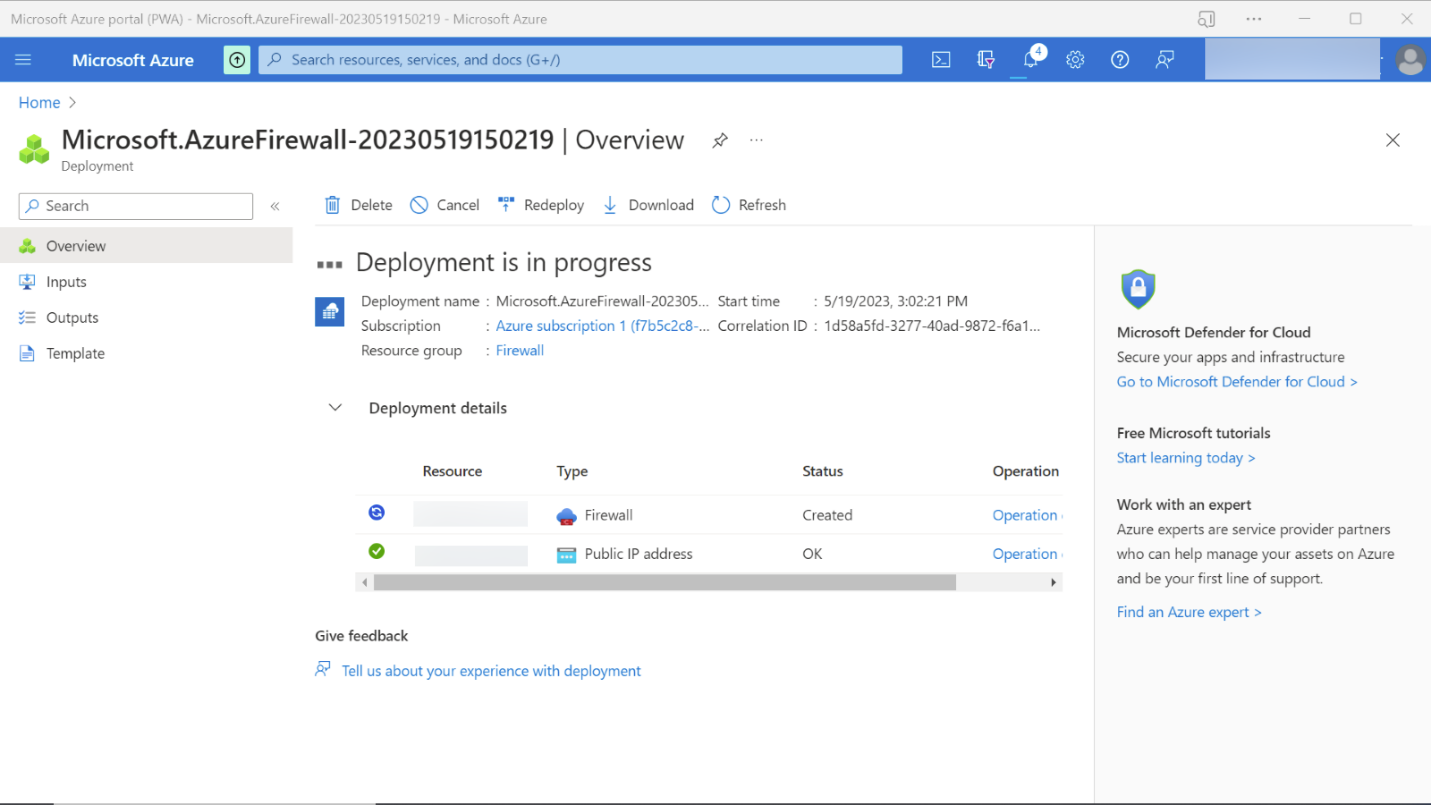
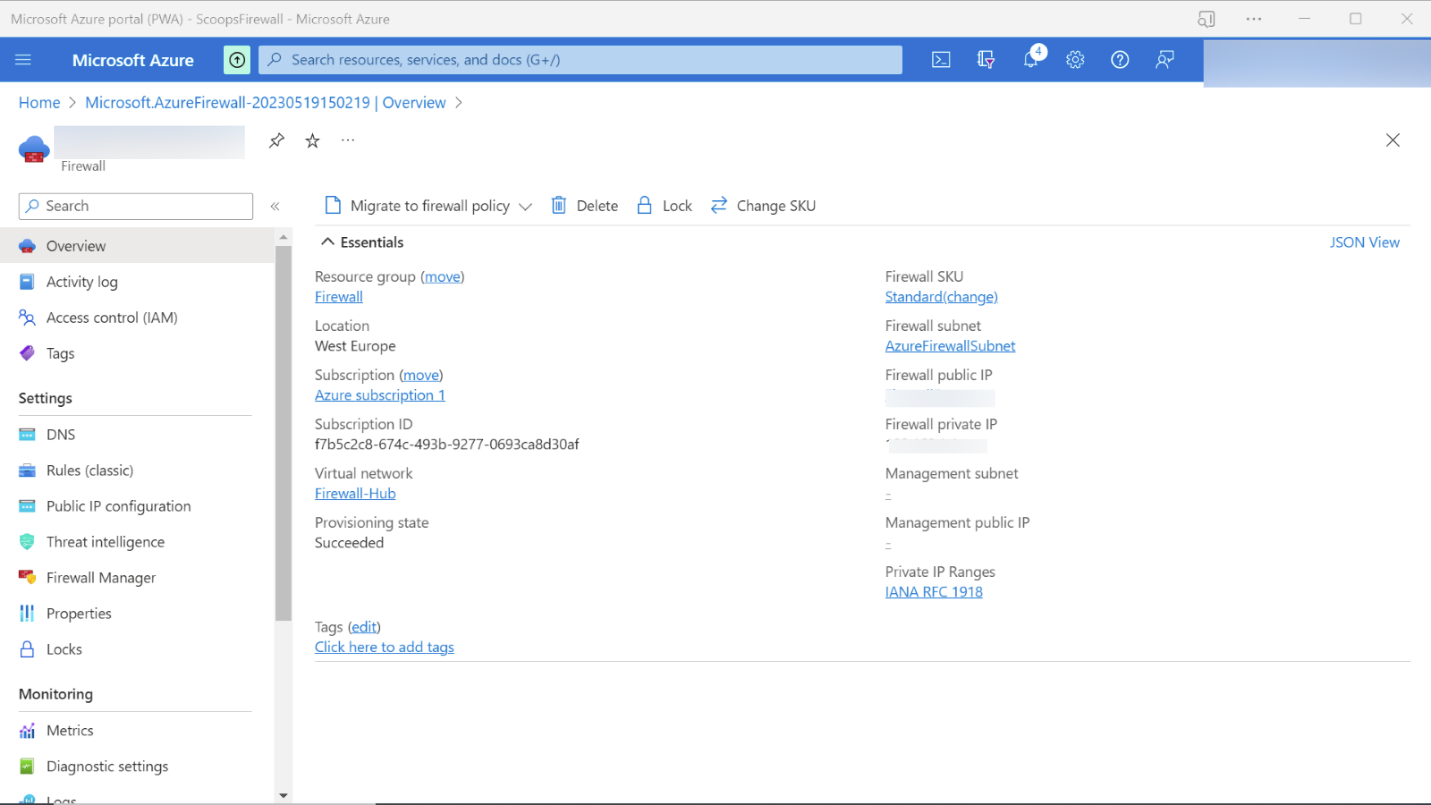
Step 17- Now set the SKU and V-net.



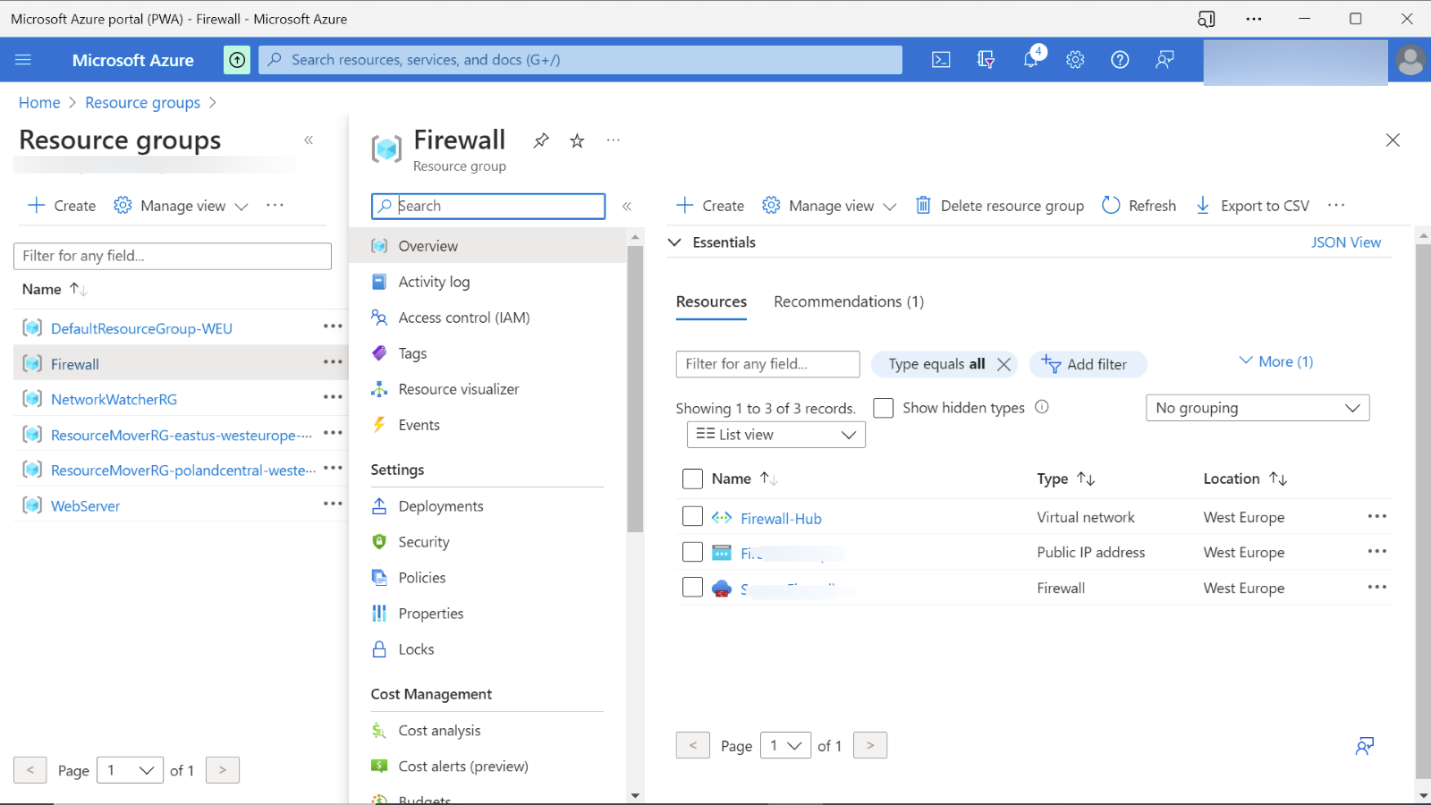
Step 18- This is the overview of our firewall.



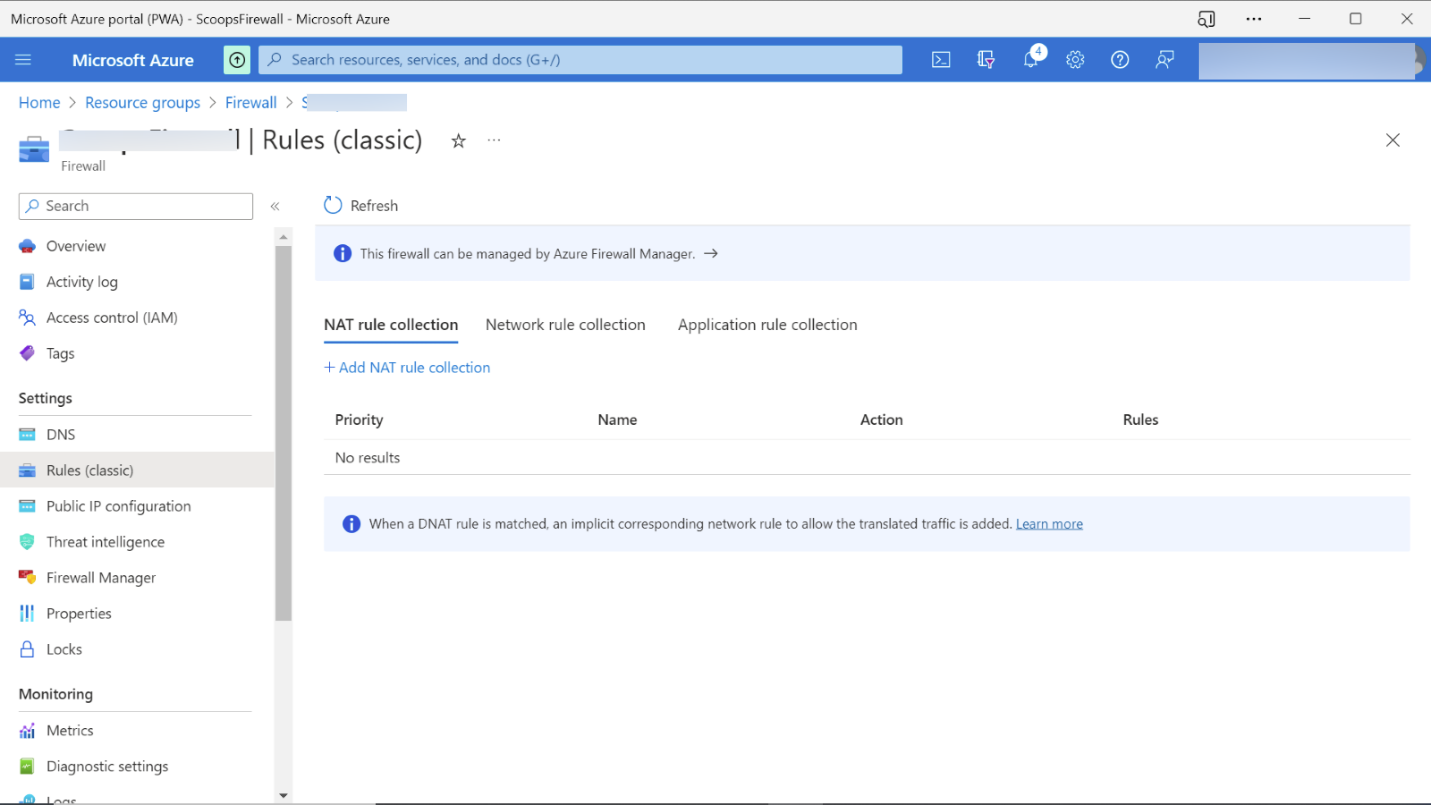
Step 19- Your Firewall is now deployed.

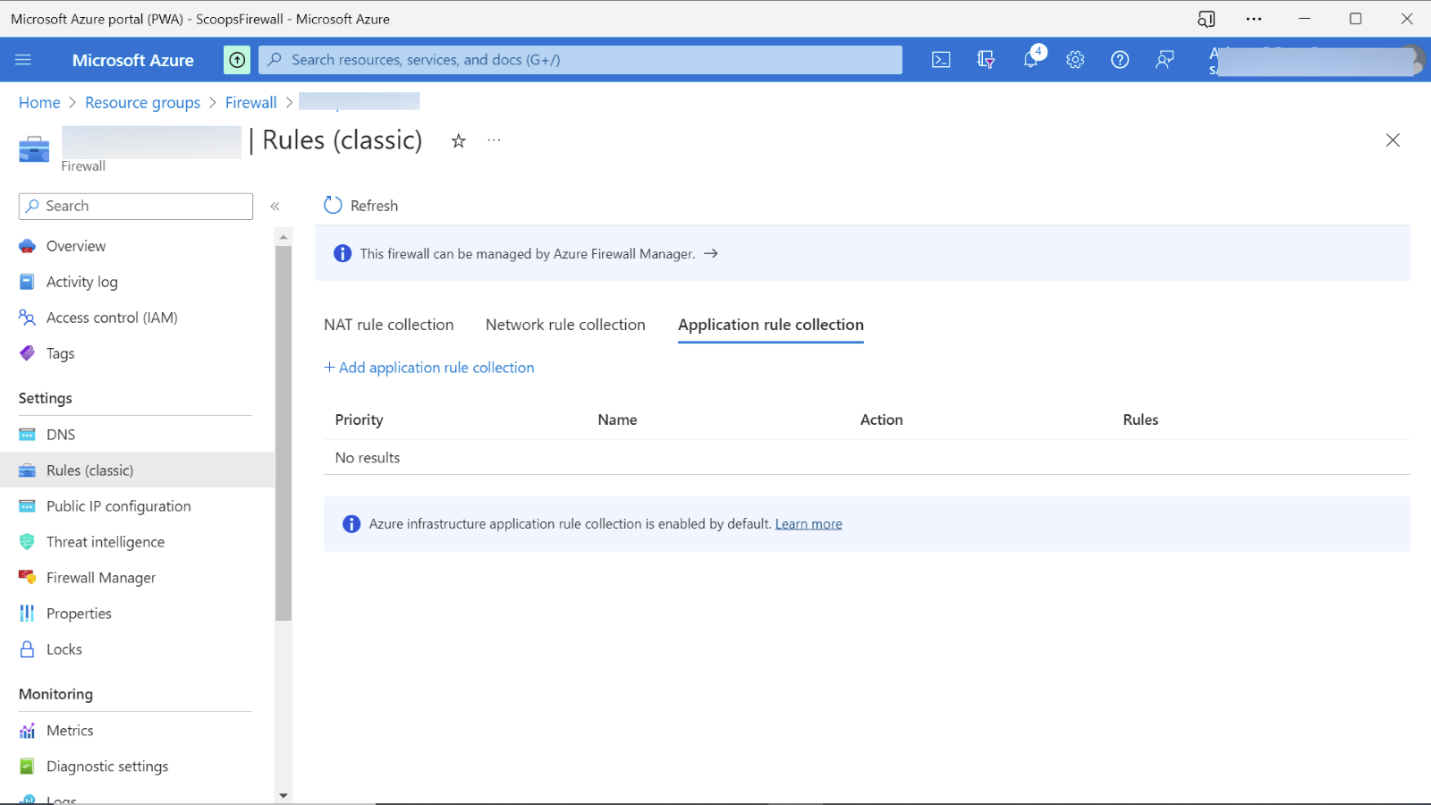
Step 20- Now we are going to set some Firewall rules. To do the same go to the Firewall Resource group.



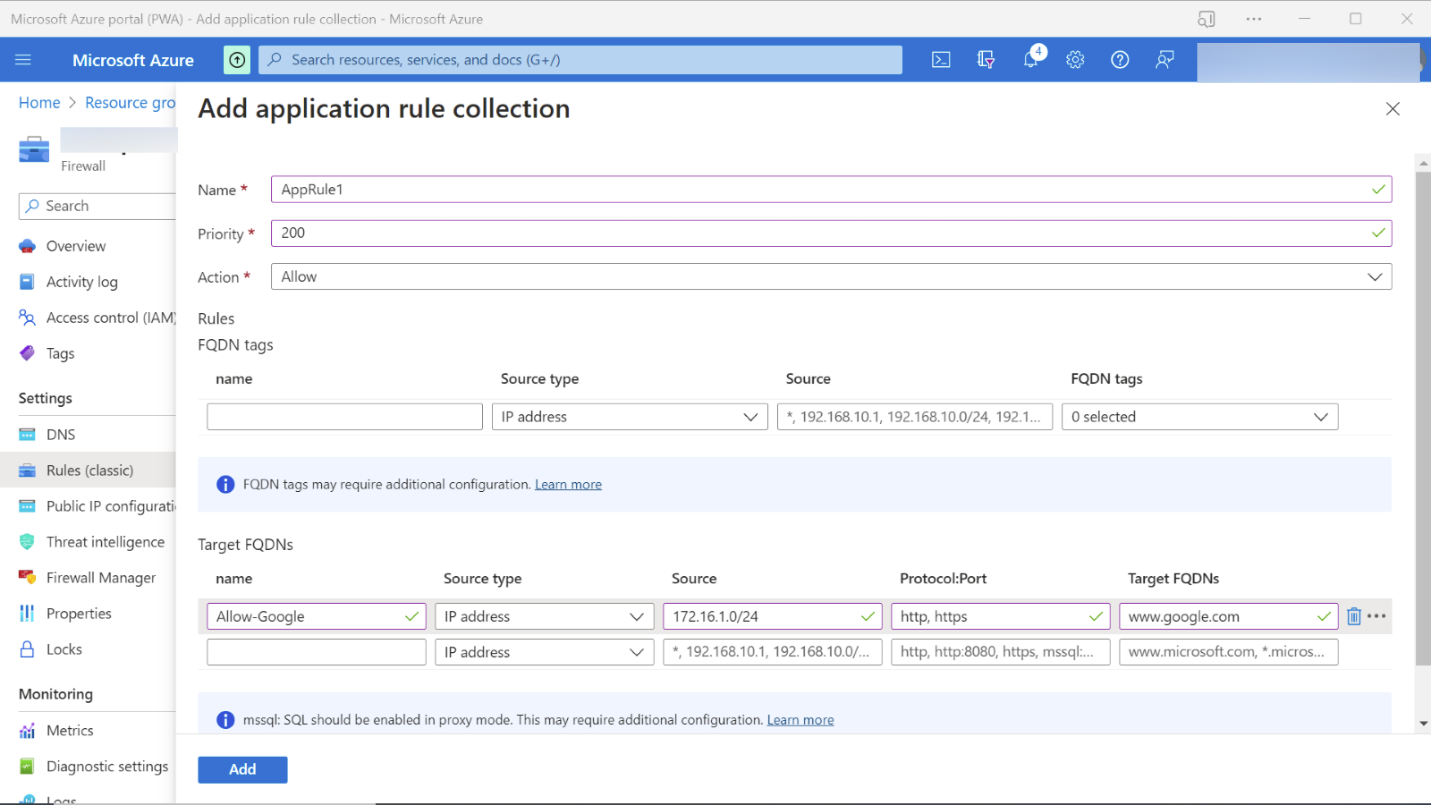
Step 21- Go to the Rule (classic) tab and create a NAT rule using NAT rule collection option.



Step 22- Now configure the Network and Application rule collection.



Step 23- Now add the name of Application rule and set the priority and Action.



Step 24- After adding it we have succesfully set the Firewall rules.

