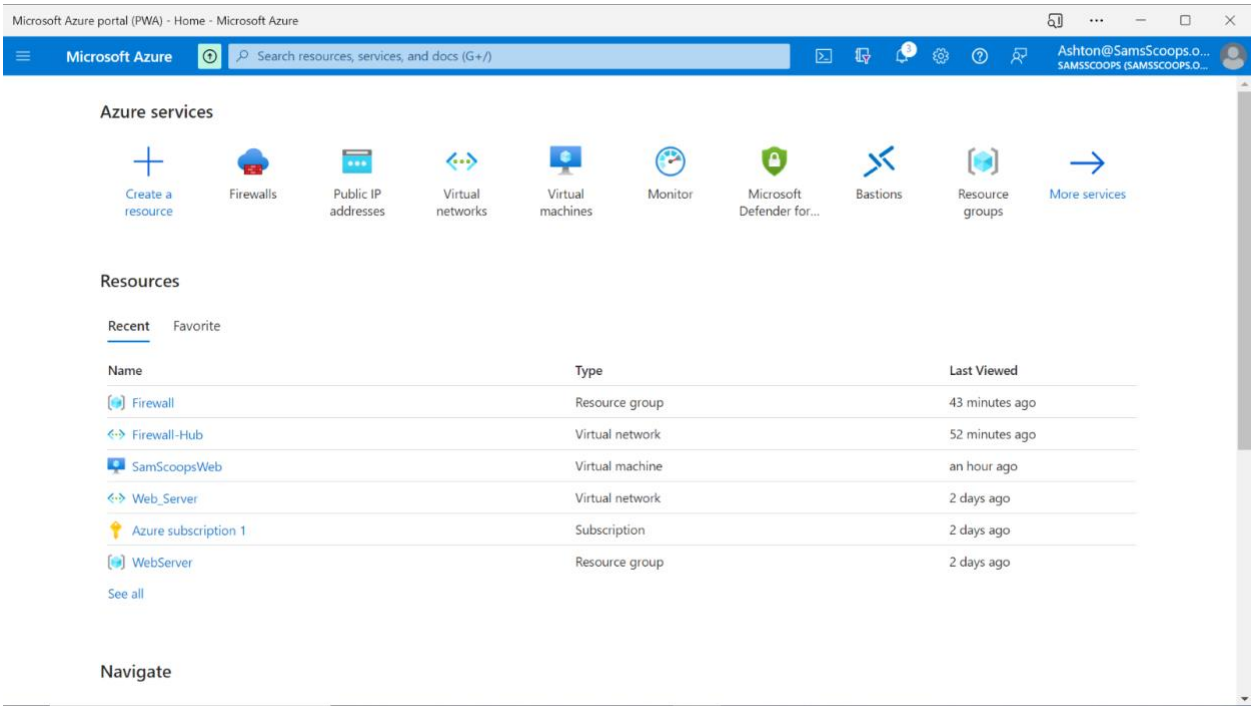
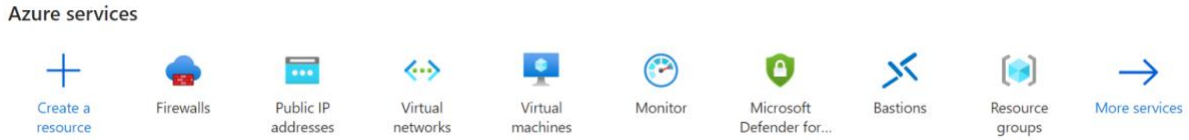
Azure Firewall Deployment and Configuration

Step 1: Firewall deployment

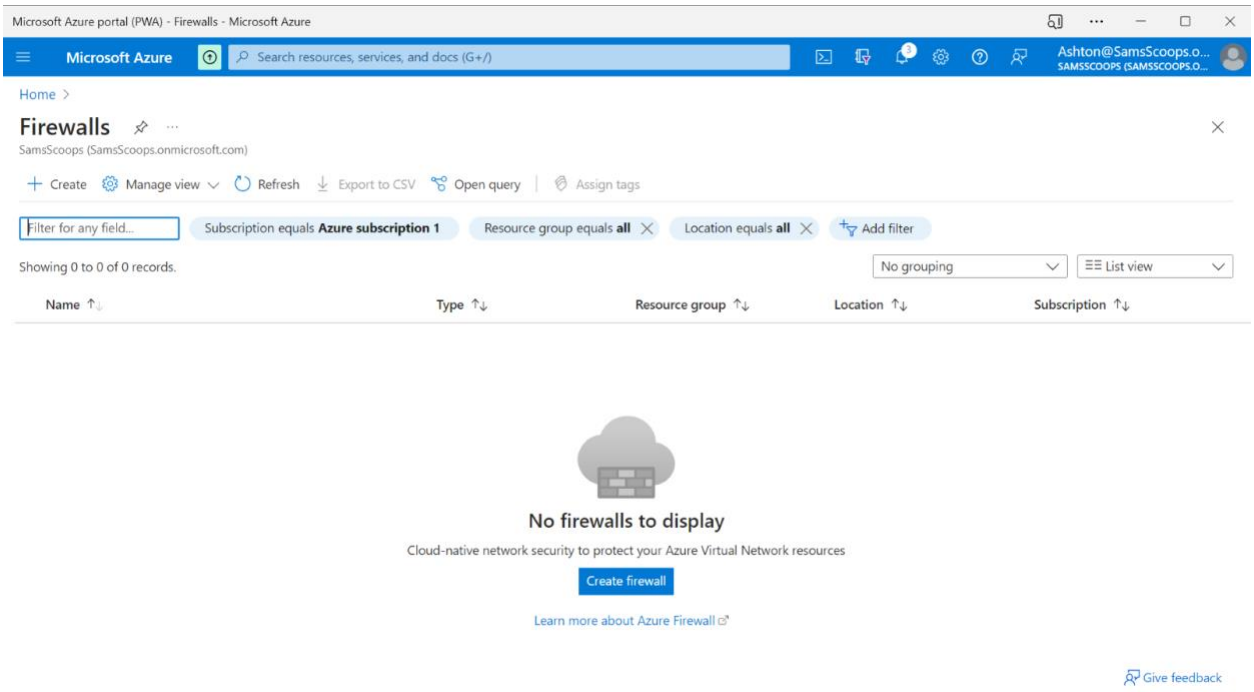
1. Sign into your Azure subscription from the Azure portal.



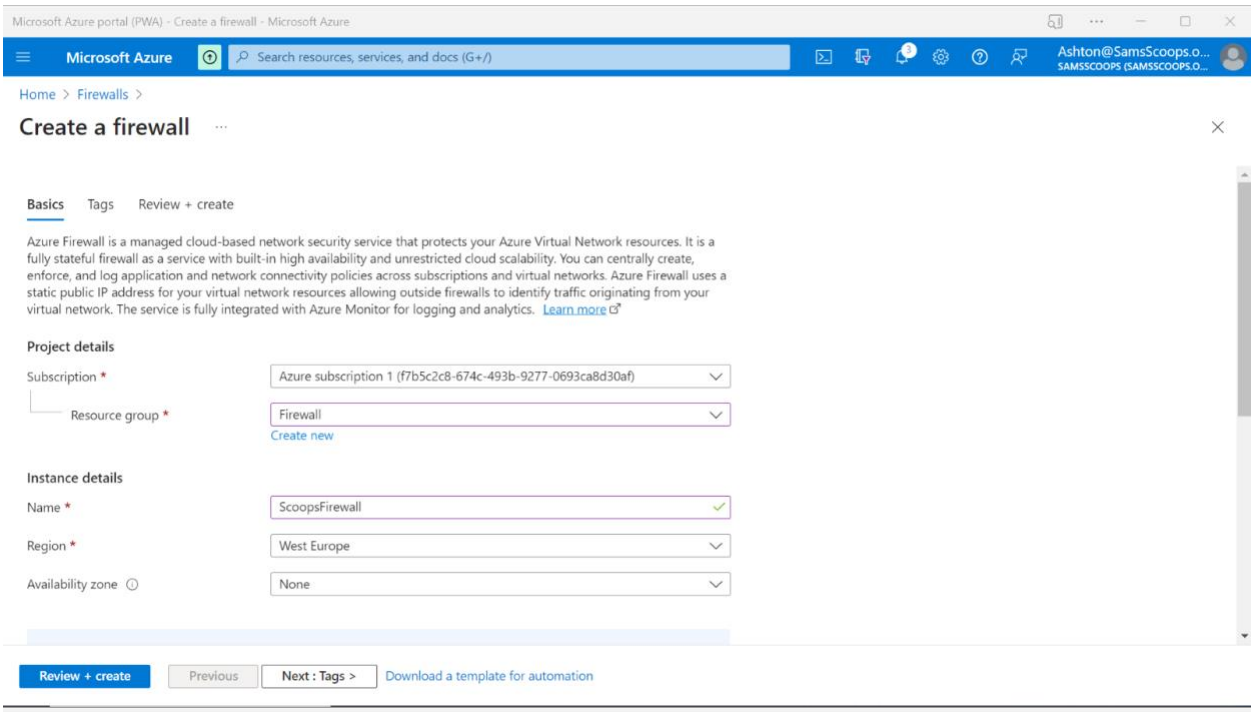
2. On the Azure home page select **Firewalls** under the Azure services bar.

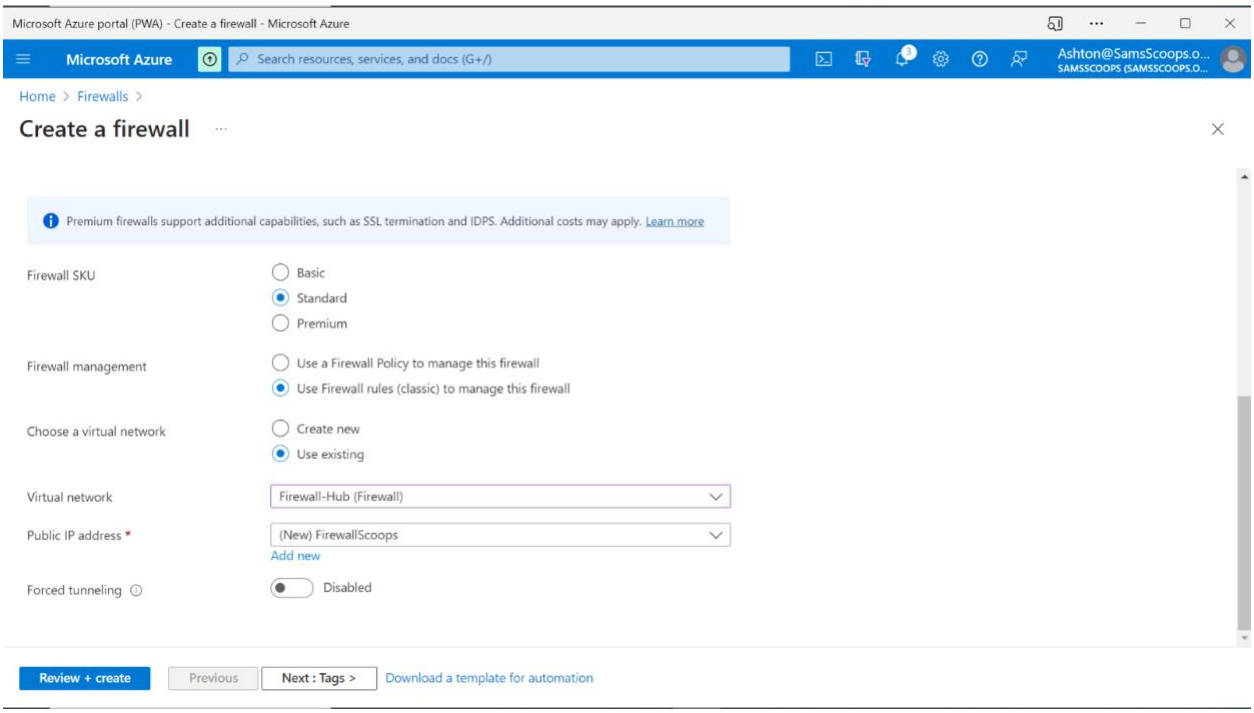


3. Select **Create Firewall**.

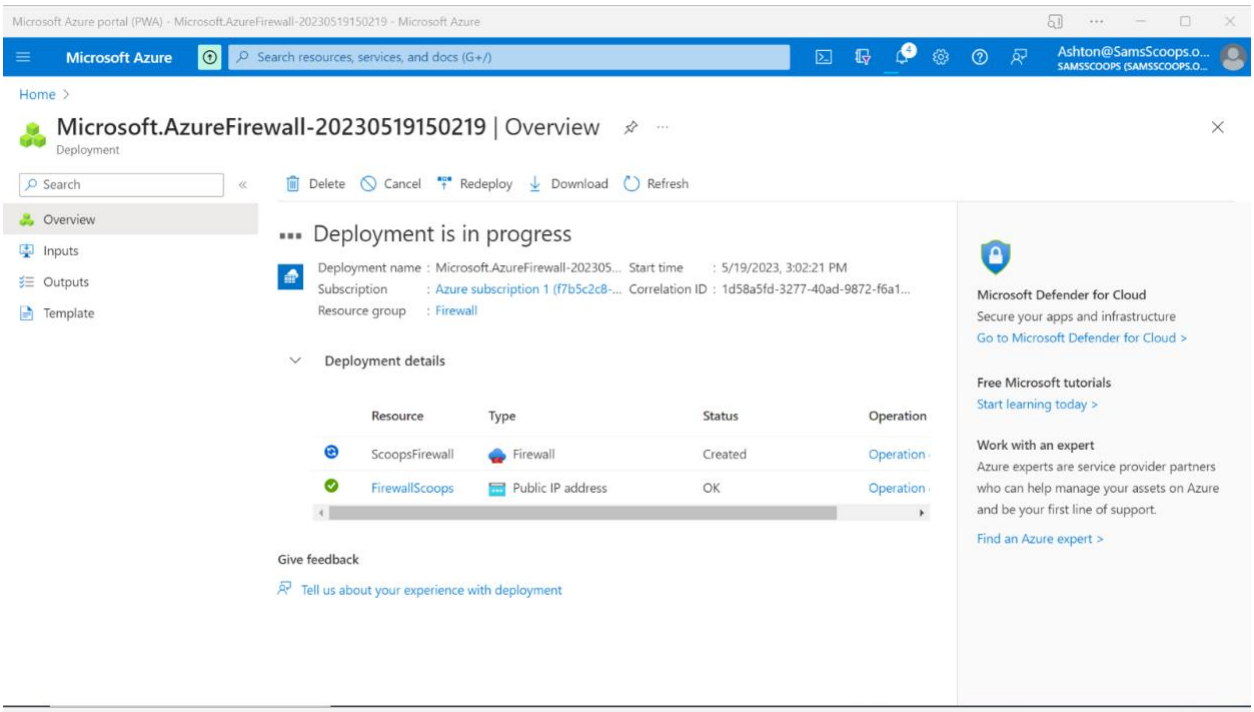


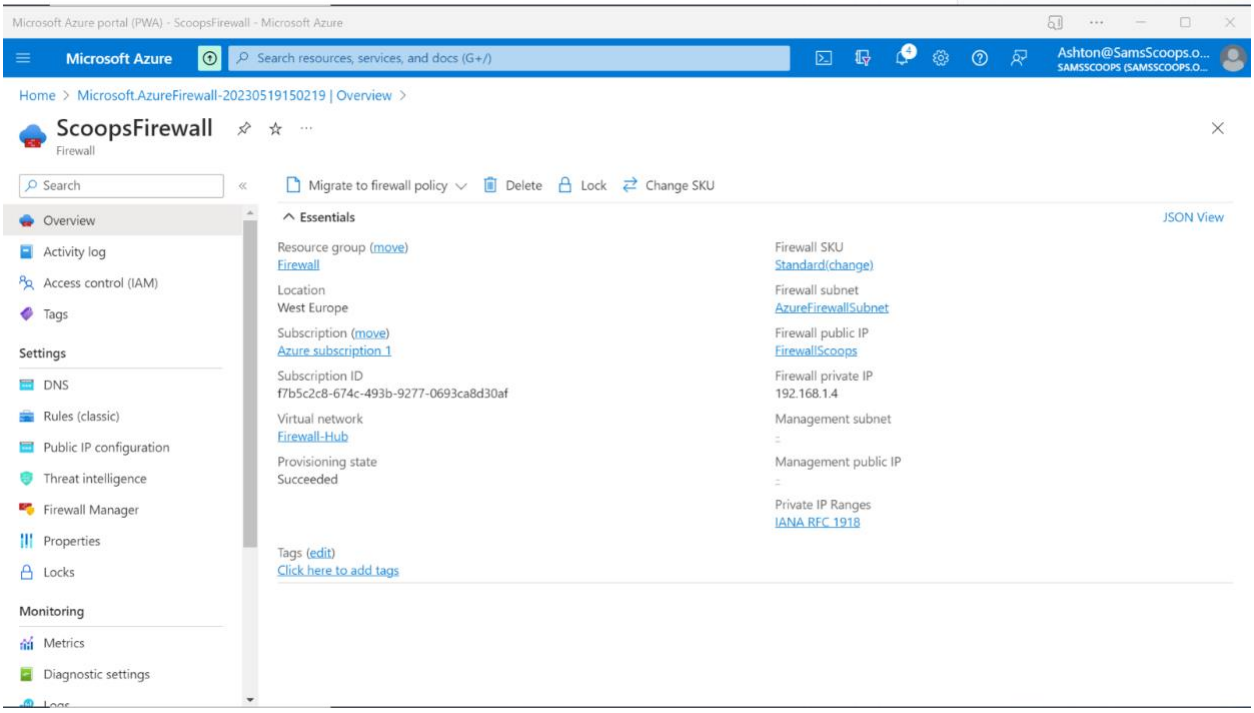
1. Subscription: Select your subscription.
2. For the resource group, select the **Firewall** resource group from the dropdown, created in the earlier activity.
3. Give the firewall instance the name "ScoopsFirewall".
4. For the region, select the same location that you have used previously.
5. For the Firewall SKU, select **Standard** from the Firewall SKU selection boxes.
6. For Firewall management, select **Use Firewall rules (classic) to manage this firewall**.
7. For **Choose a virtual network**, select **Use existing** and select the **Firewall-Hub** network for the virtual network created in a previous activity.
8. For the Public IP address, select **Add new** and give it the name "FirewallScoops", select **OK**.





1. Select **Review + create** then **create.** The firewall will now be deployed.

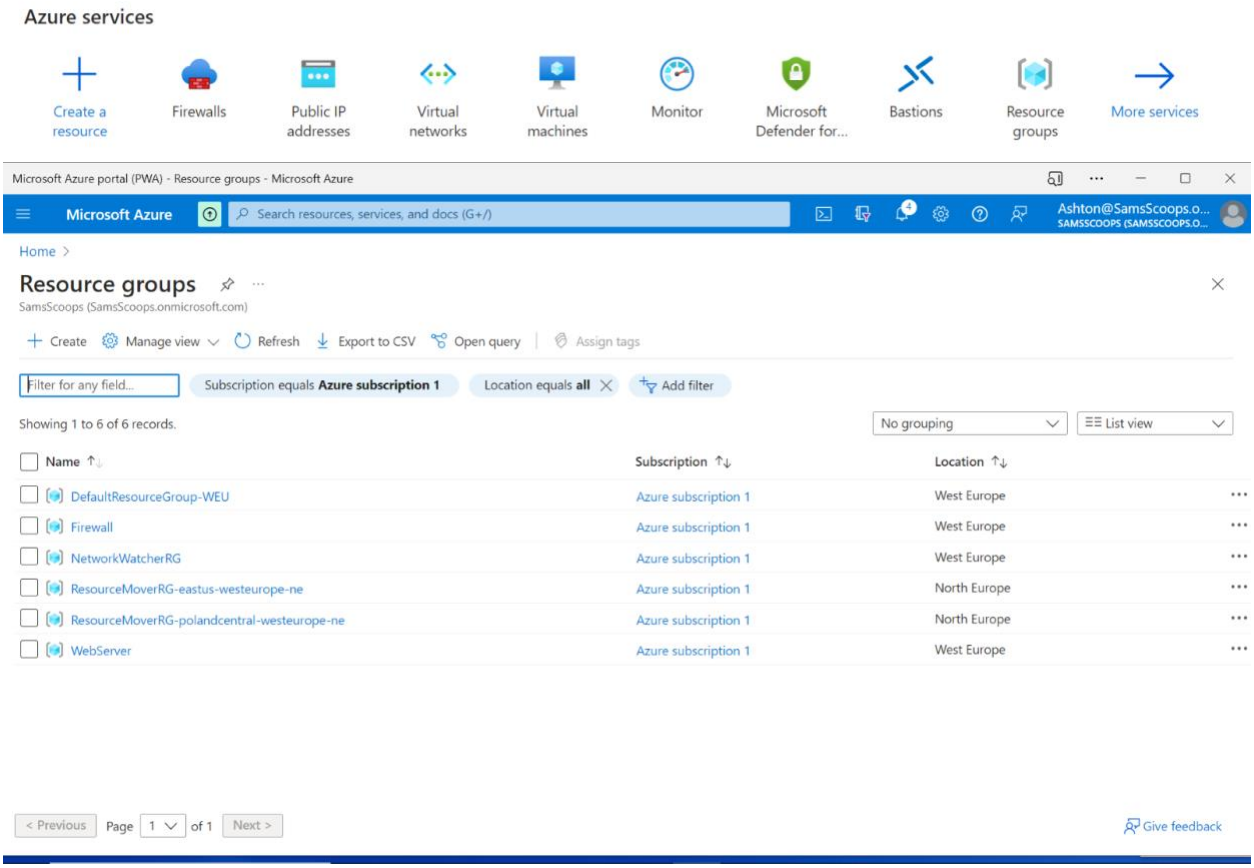




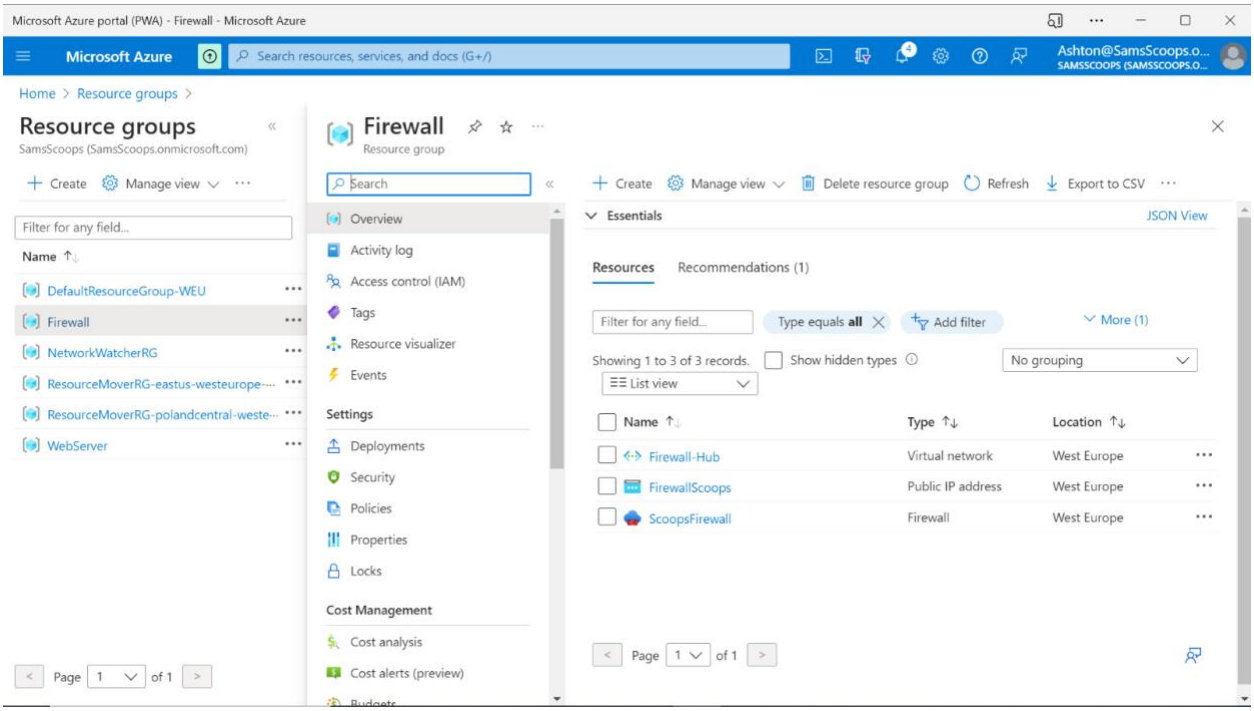
Step 2: Firewall application rules creation

The web server will need access to Google once it is set up, so you need to set up an application rule to allow outbound access. To do this, follow these steps:

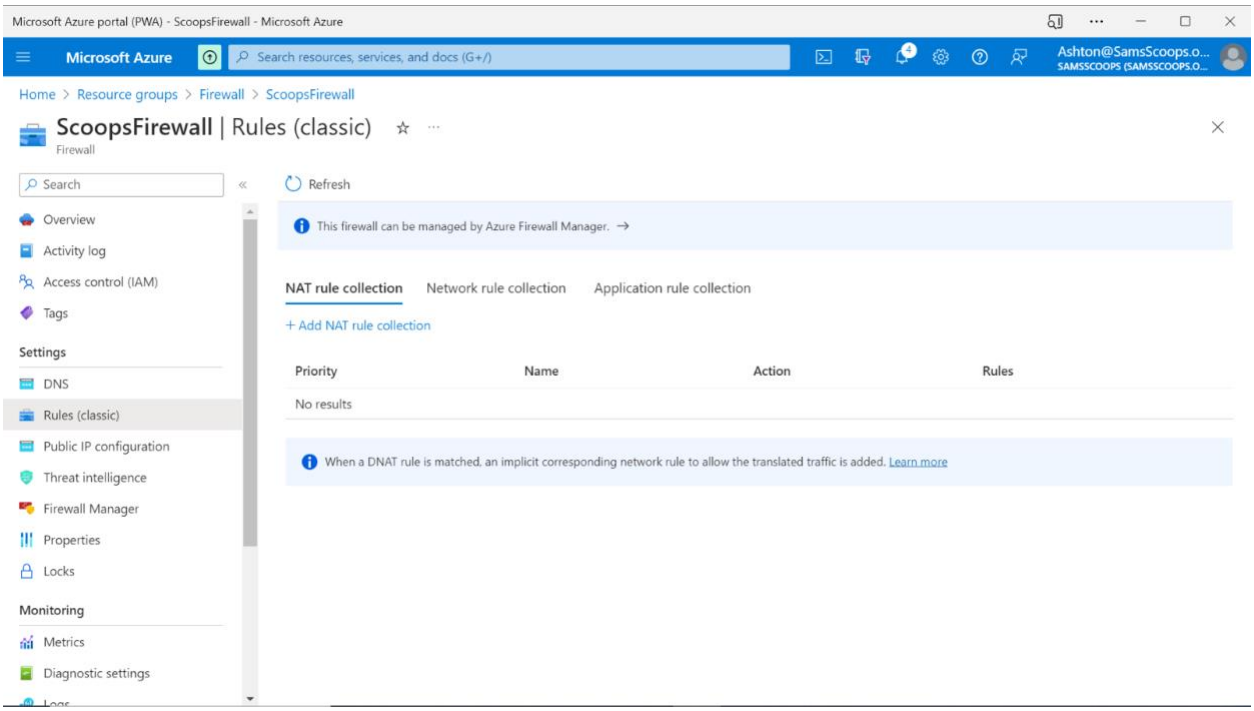
1. From the Azure services bar select **Resource groups**.



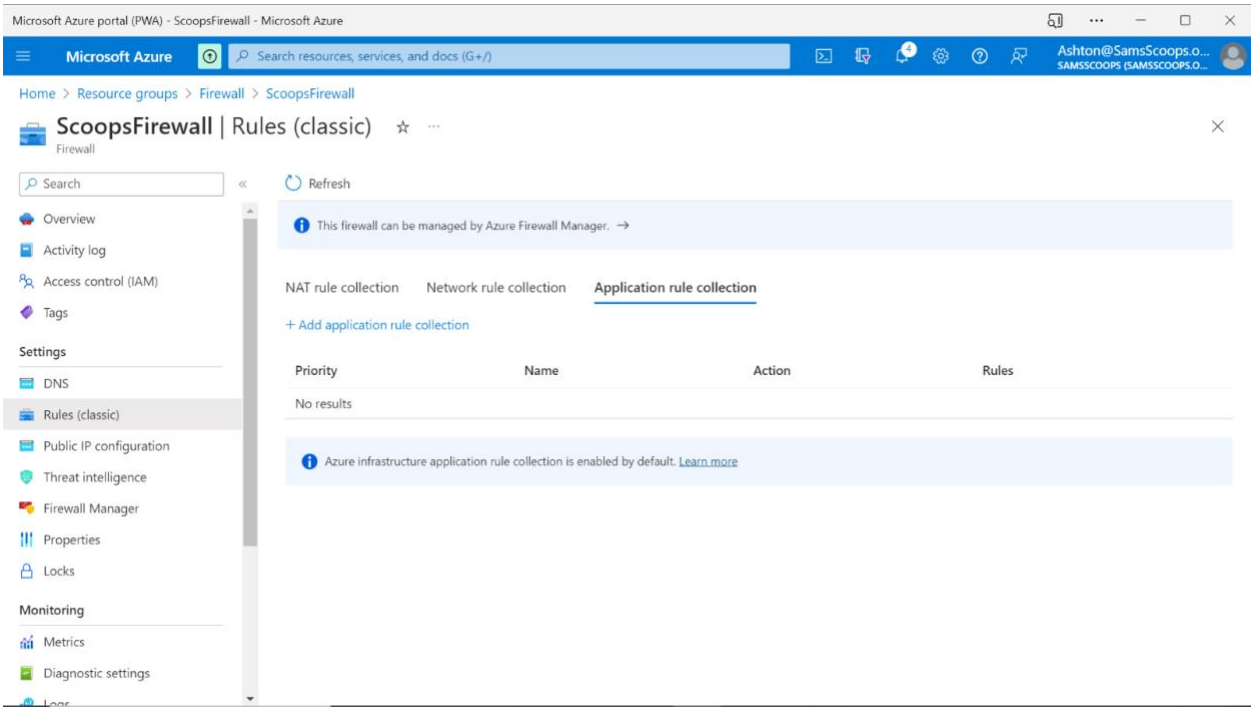
1. Open the **Firewall** resource group, and select the **ScoopsFirewall** firewall.



1. On the **ScoopsFirewall** page, under **Settings**, select **Rules (classic)**.

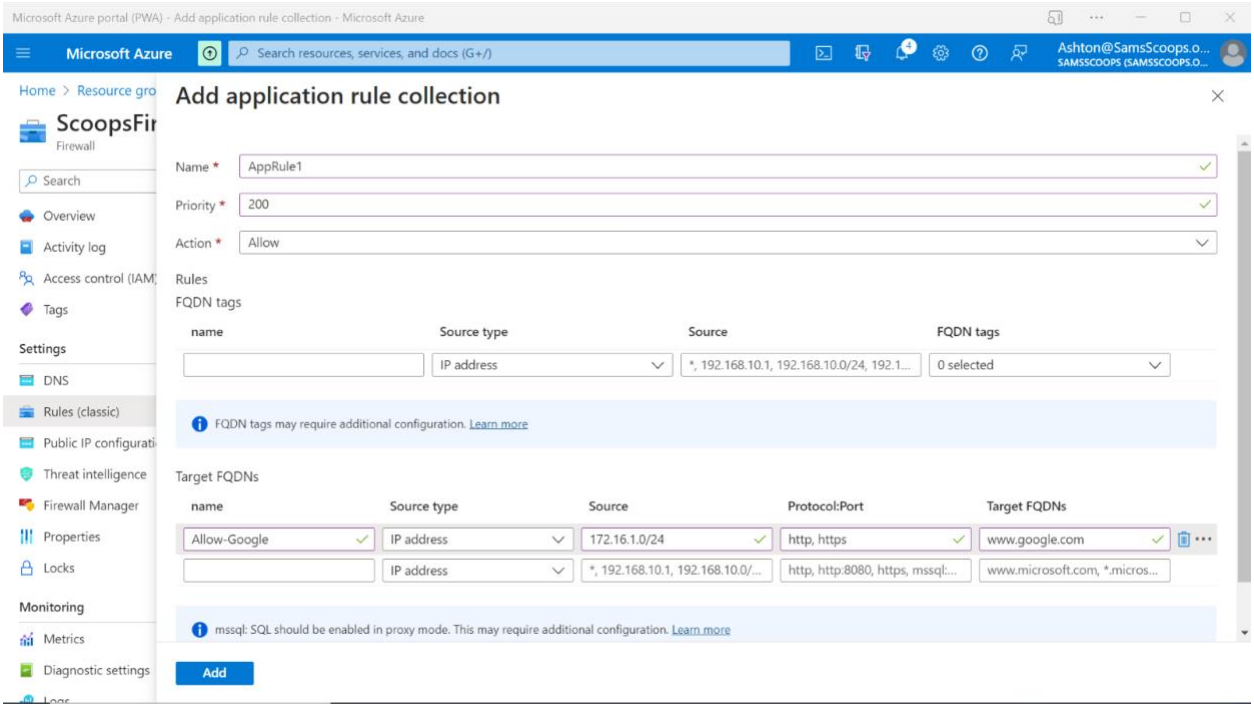


1. Select the **Application rule collection** tab.

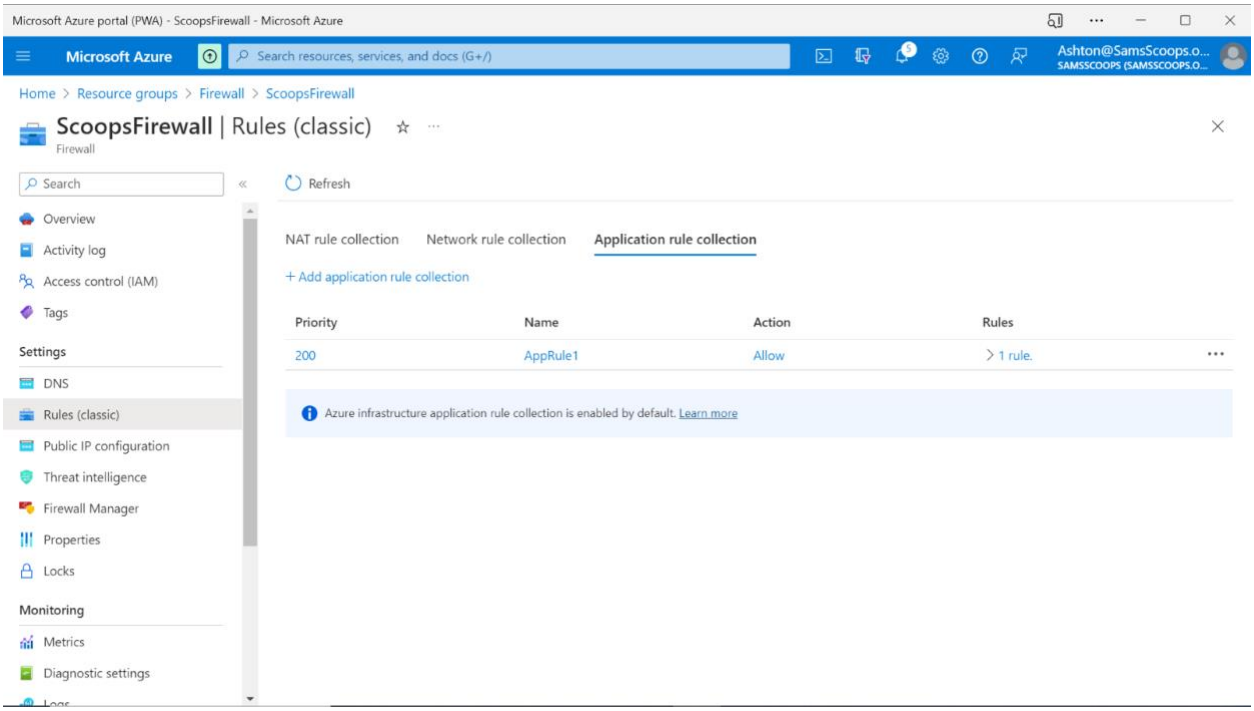


1. Select **Add application rule collection**.
2. For **Name**, type "AppRule1".
3. For **Priority**, type "200".
4. For **Action**, select **Allow**.
5. Under **Rules**, **Target FQDNs**, for **Name**, type "Allow-Google".
6. For **Source type**, select **IP address**.

7. Type **172.16.1.0/24** for the source.
8. For **Protocol:port**, type "http, https".
9. For **Target FQDNS**, type "www.google.com".



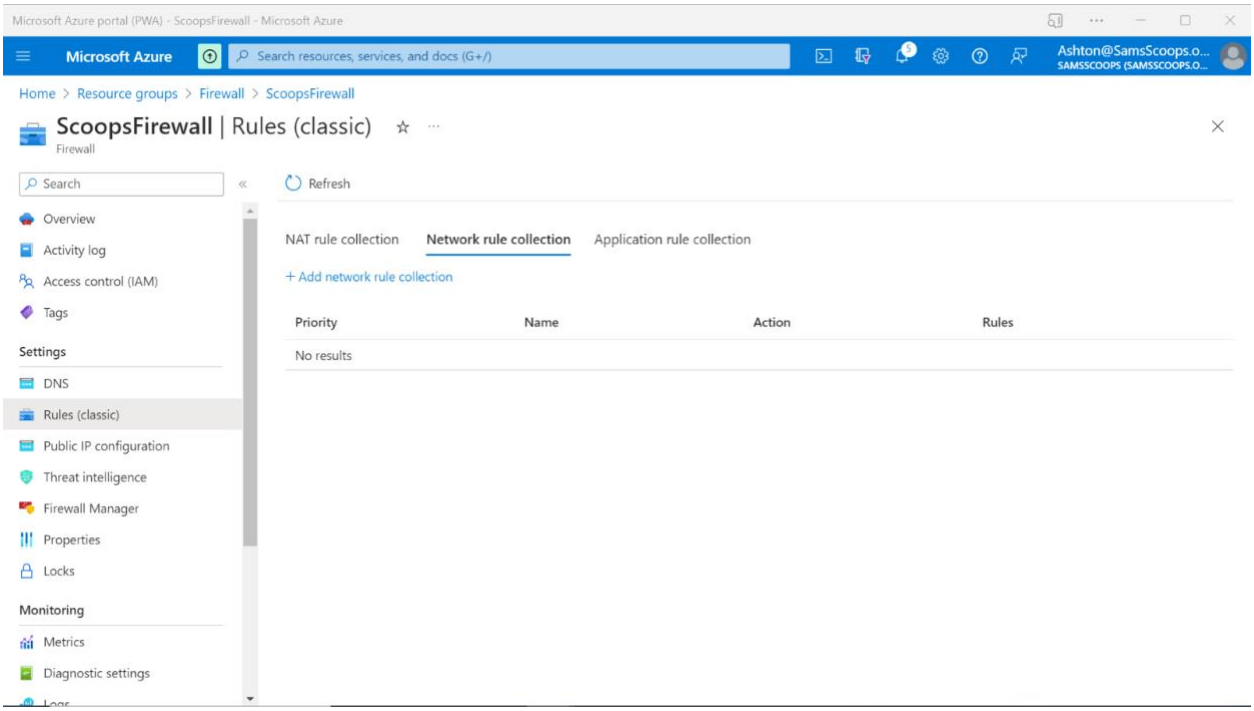
1. Select **Add** and after a short time the rule will be created.



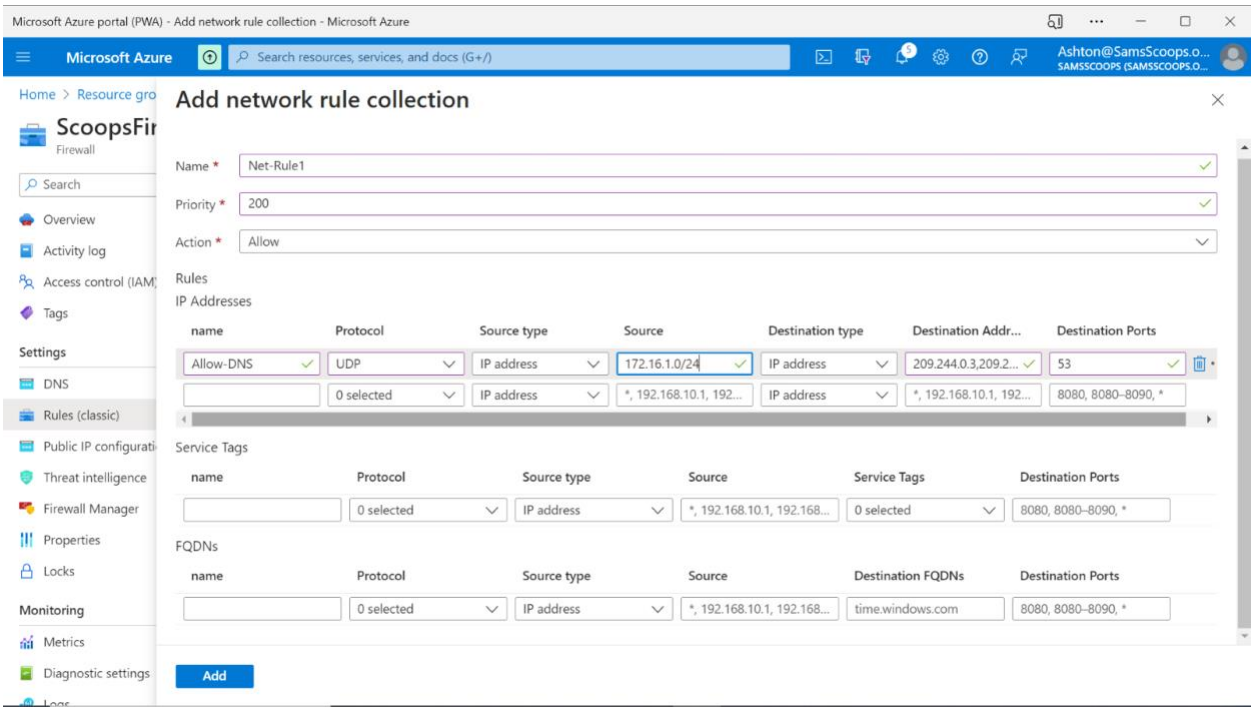
Step 3: Firewall network rule creation

The web server will also need to use DNS to resolve IP addresses so you need to create a network rule to allow this. Follow these steps to do this:

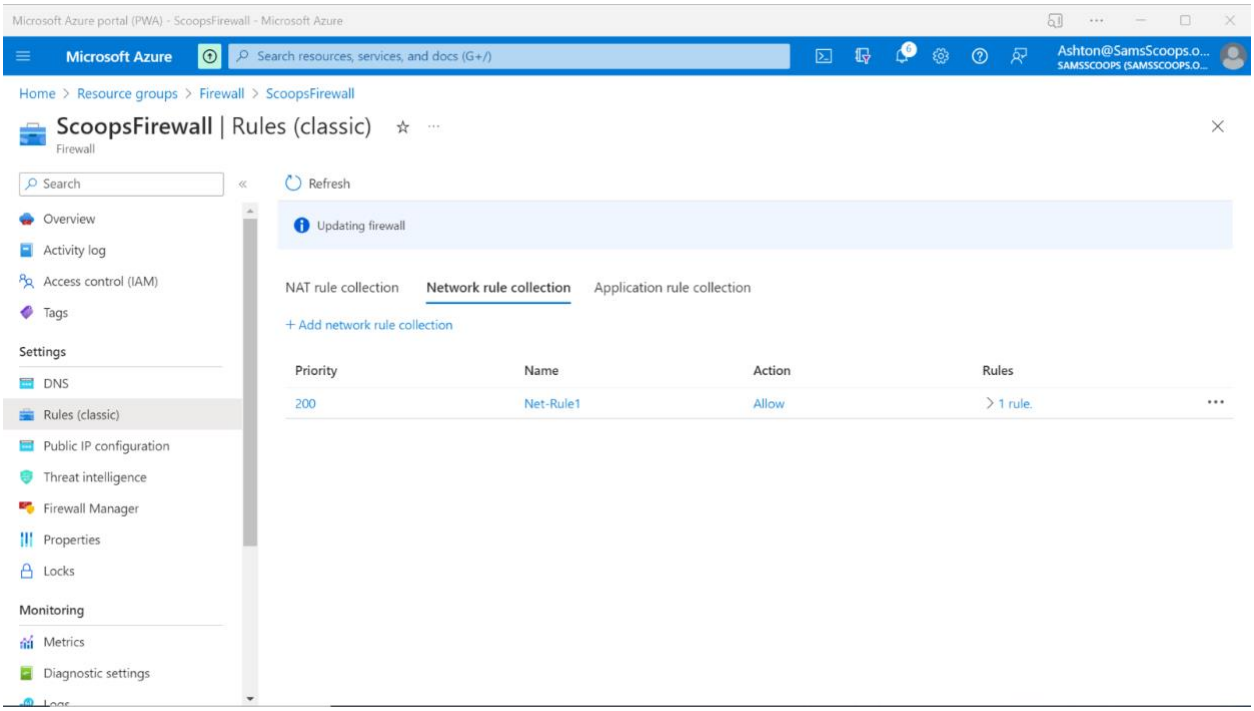
1. Select the **Network rule collection** tab.
2. Select **Add network rule collection**.



1. For **Name**, type "Net-Rule1".
2. For **Priority**, type "200".
3. For **Action**, select **Allow**.
4. Under **Rules**, **IP addresses**, for **Name**, type "Allow-DNS".
5. For **Protocol**, select **UDP**.
6. For **Source type**, select **IP address**.
7. Type **172.16.1.0/24** for the **Source**.
8. For **Destination type** select **IP address**.
9. For **Destination address**, type **209.244.0.3,209.244.0.4** (These are public DNS servers operated by Level3).
10. For **Destination Ports**, type "53".



1. Select **Add**.

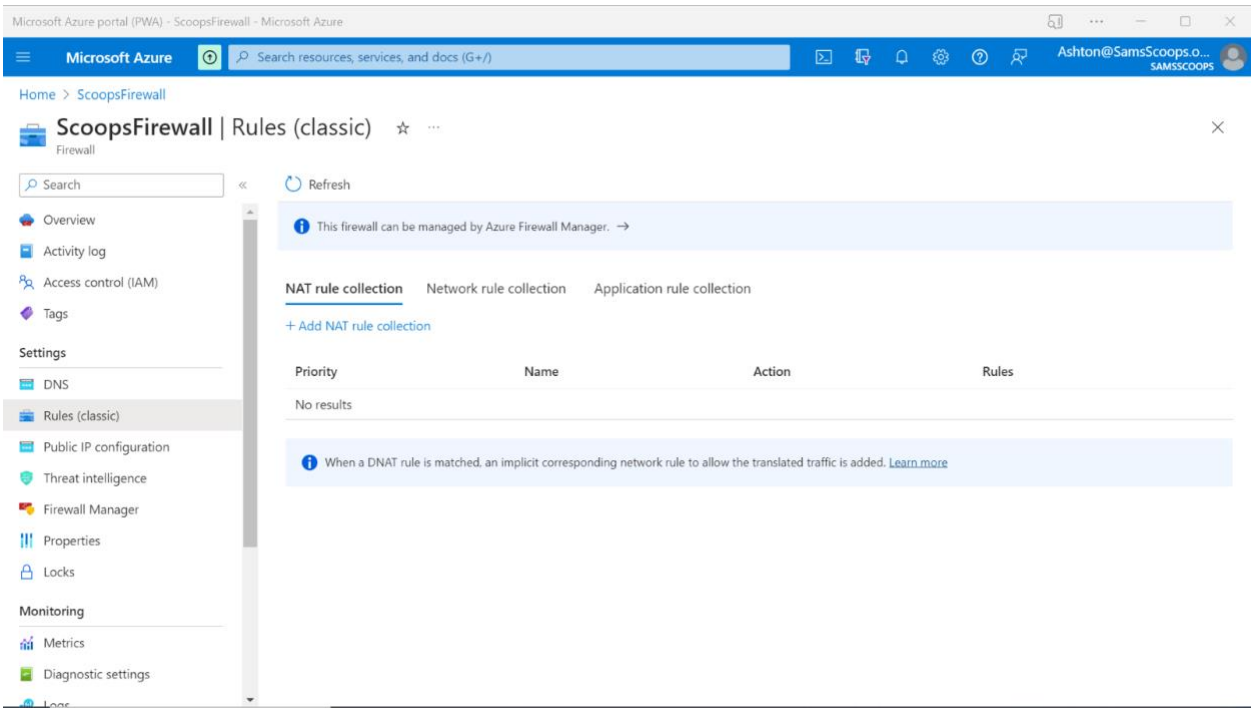


Step 4: Firewall NAT rules creation

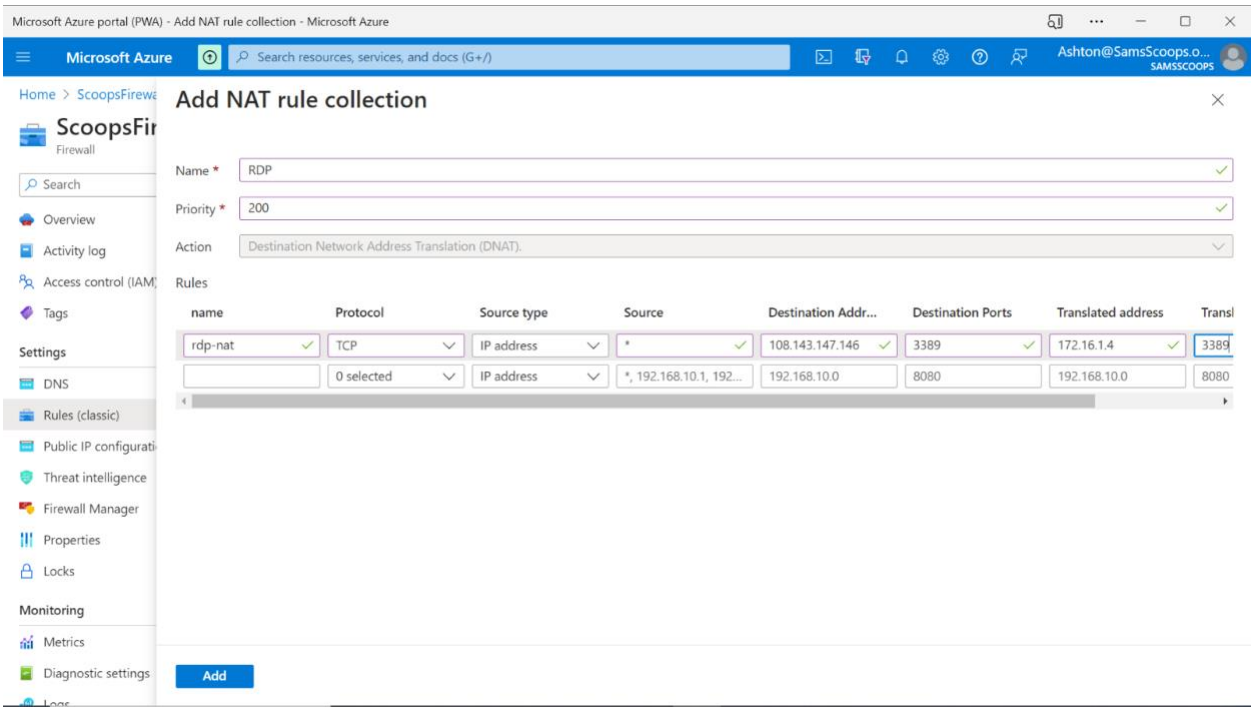
To allow the web developer to set up the web server you need to provide remote access to the VM. Follow these steps to create a destination NAT rule for RDP:

1. Select the **NAT rule collection** tab.

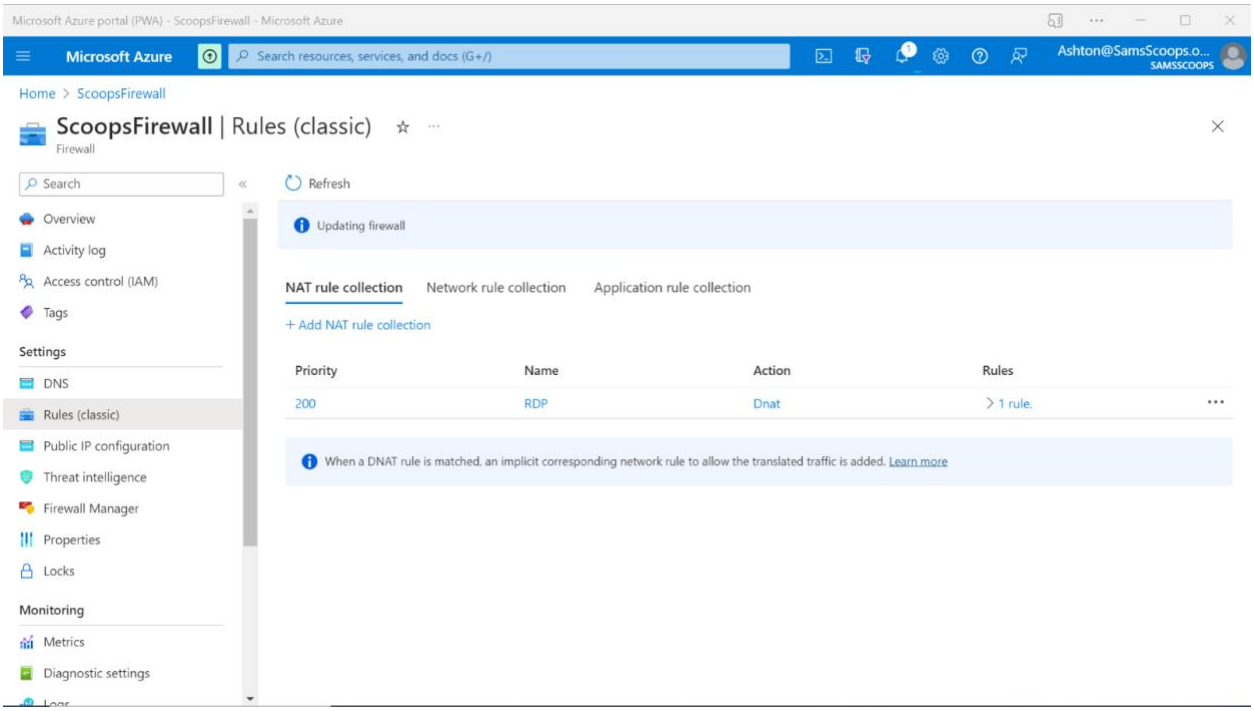
2. Select **Add NAT rule collection**.



1. For **Name**, type " rdp".
2. For **Priority**, type "200".
3. Under **Rules**, for **Name**, type "rdp-nat2".
4. For **Protocol**, select **TCP**.
5. For **Source type**, select **IP address**.
6. Type "*.(* = anything)" for the **Source**.
7. For **Destination address**, type the firewall public IP address.
8. For **Destination Ports**, type "3389".
9. For **Translated address**, type the **SamScoopsWeb** virtual machines private IP address.
10. For **Translated port**, type "3389".



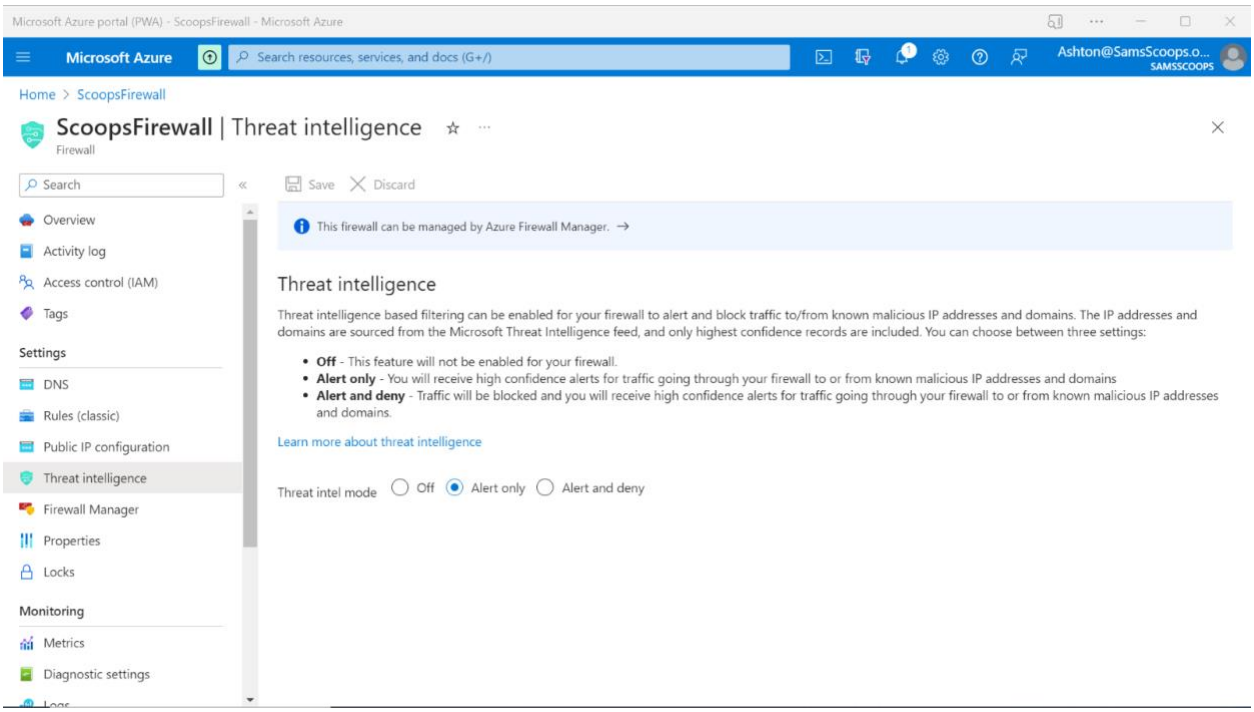
1. Select **Add**.



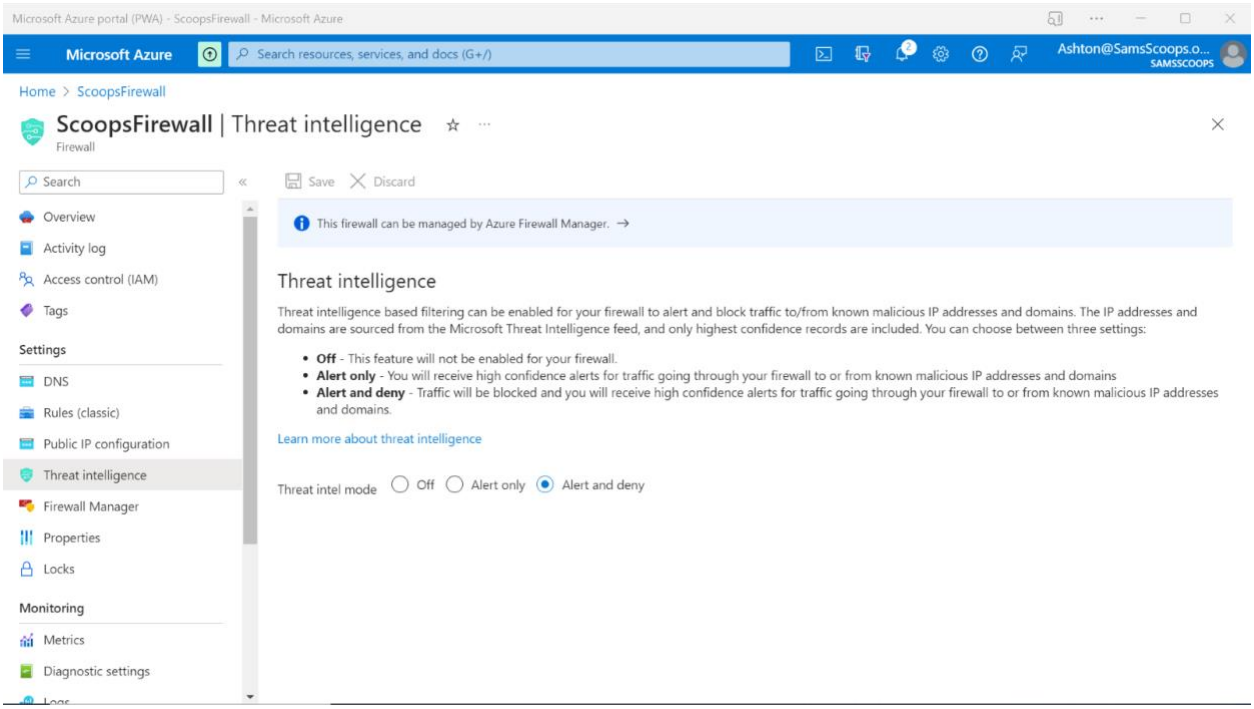
Step 5: Advanced threat protection

Earlier you learned that one of the great advantages of using the Azure Standard Firewall is that you can create rules automatically for threat using Threat Intelligence. By by default the firewall is set to only create threat alerts. Follow these steps to enable the alert and deny option.

1. On the **ScoopsFirewall** page, under **Settings**, select **Threat intelligence**.



1. For **Threat intel mode** select **Alert and deny**.



1. Select **Save**.