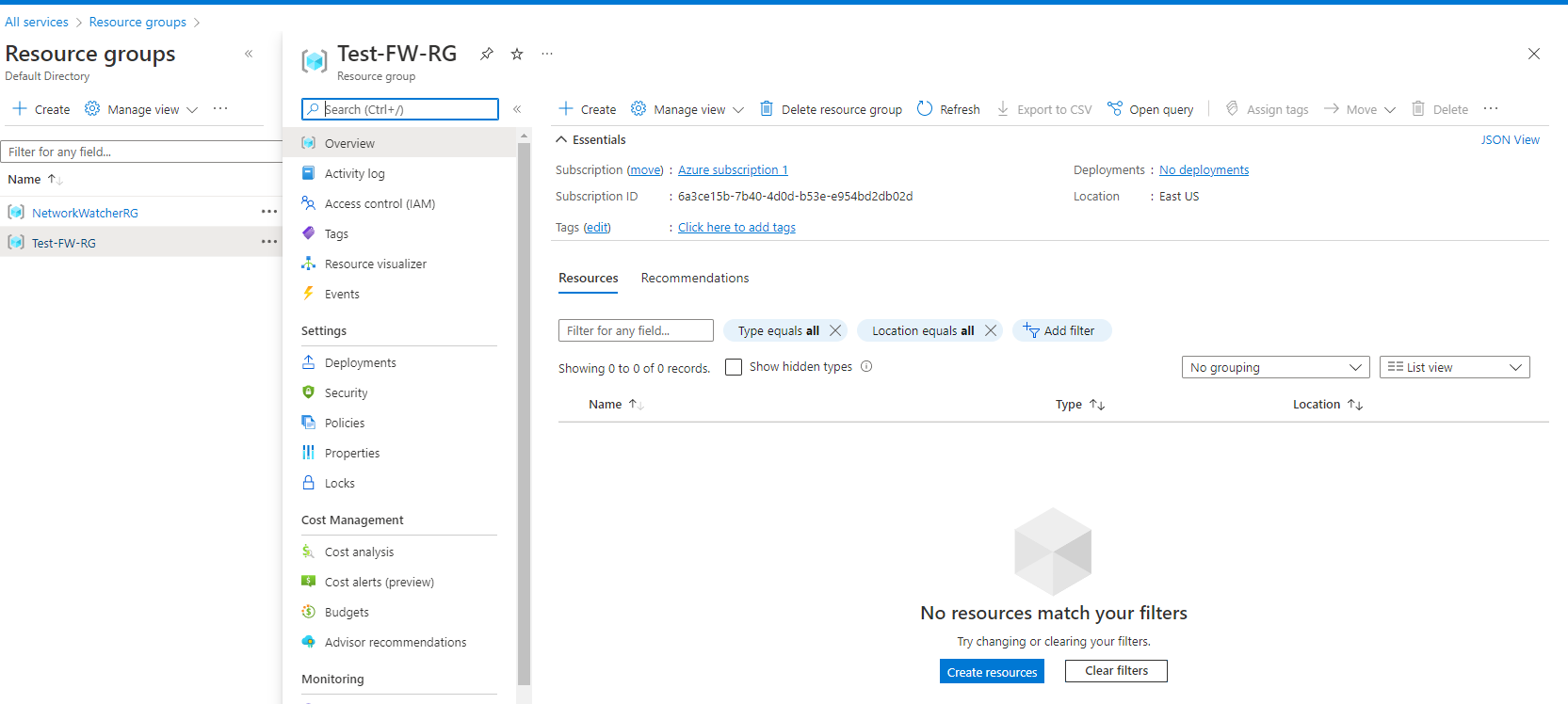
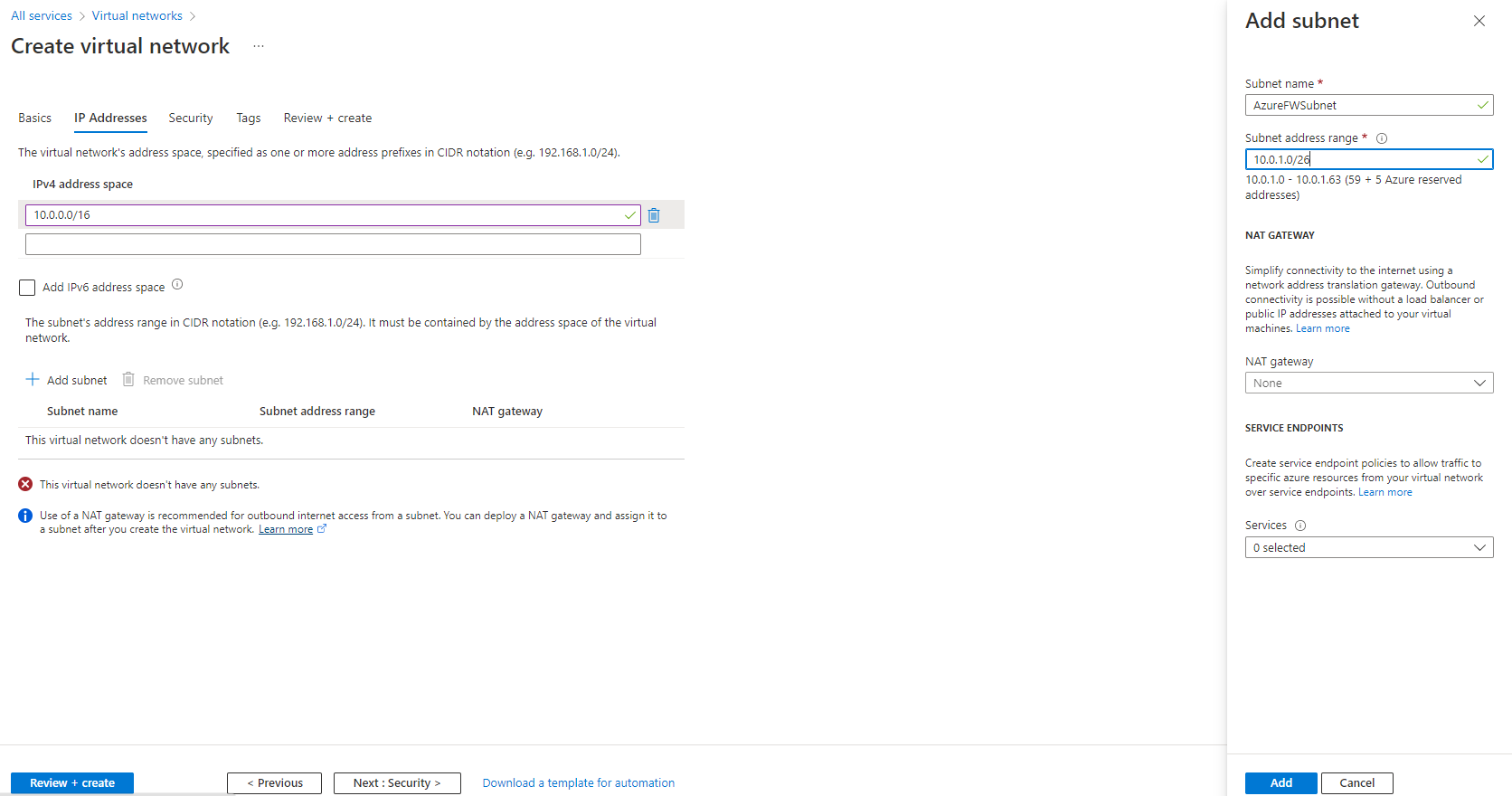
Deploying and Configuring Azure Firewall using Azure Portal

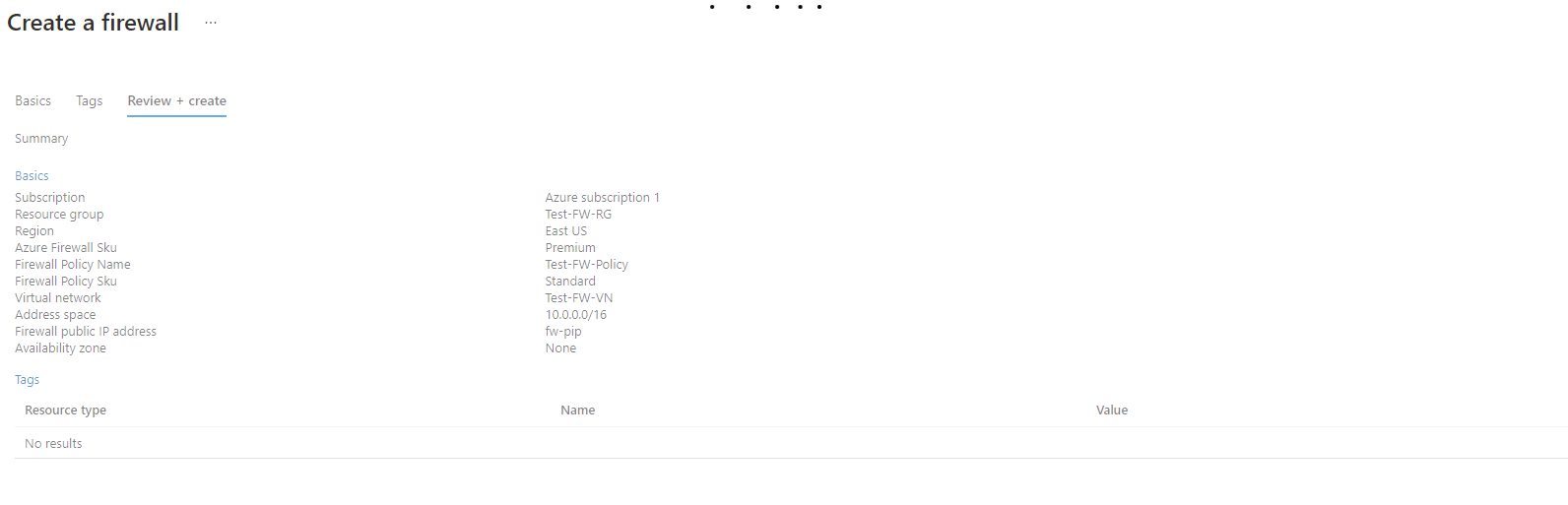
Objective: Create a test environment with a working firewall.



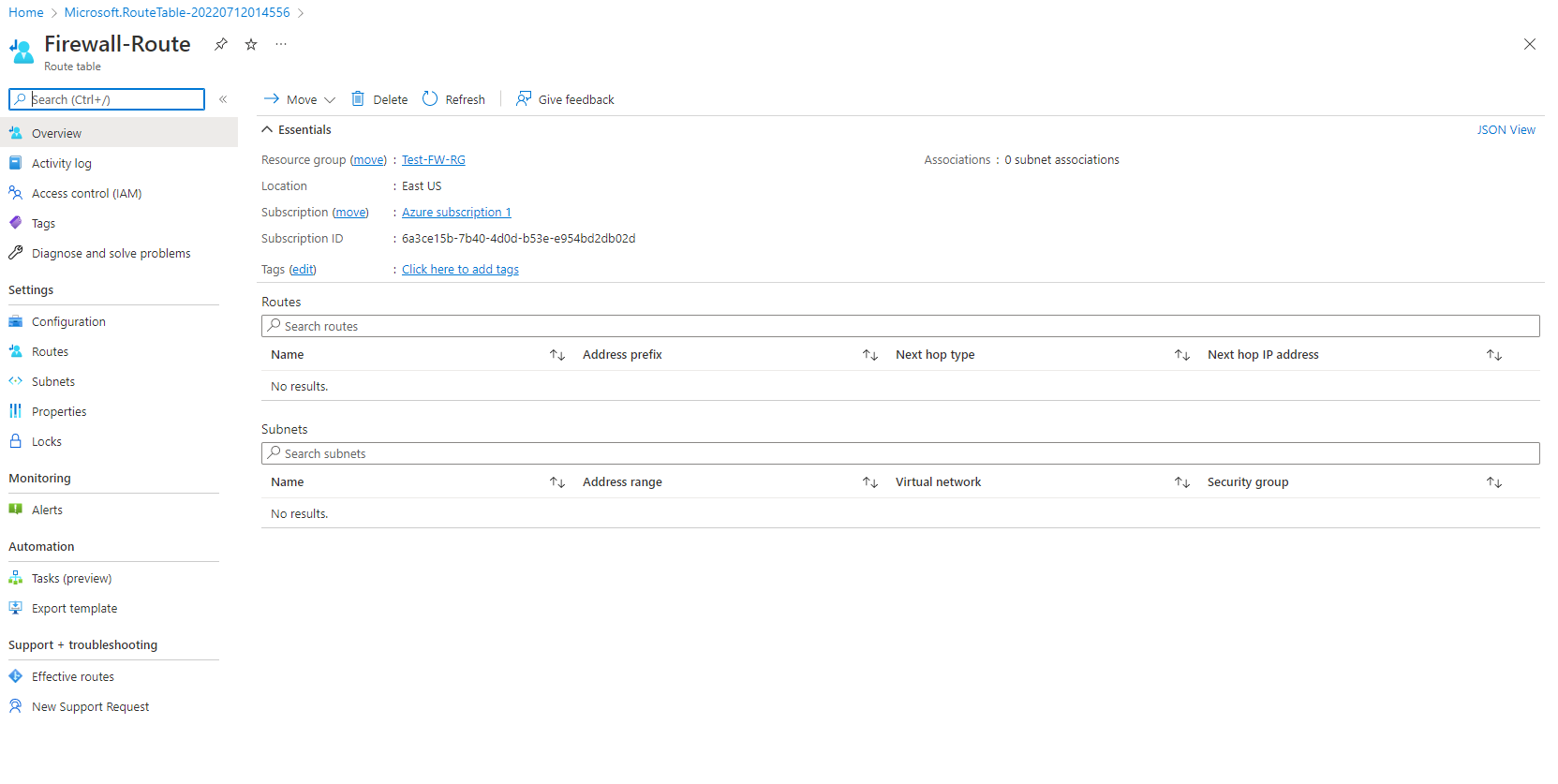
* To begin this project, I had to create an object to house all project related services and applications. Therefore, that object is a resource group which I labeled as Test-FW-RG
  + Note: To create a resource group; In Azure portal search for resource groups, create new, fill out the form with your subscription, group name and location, review and create.



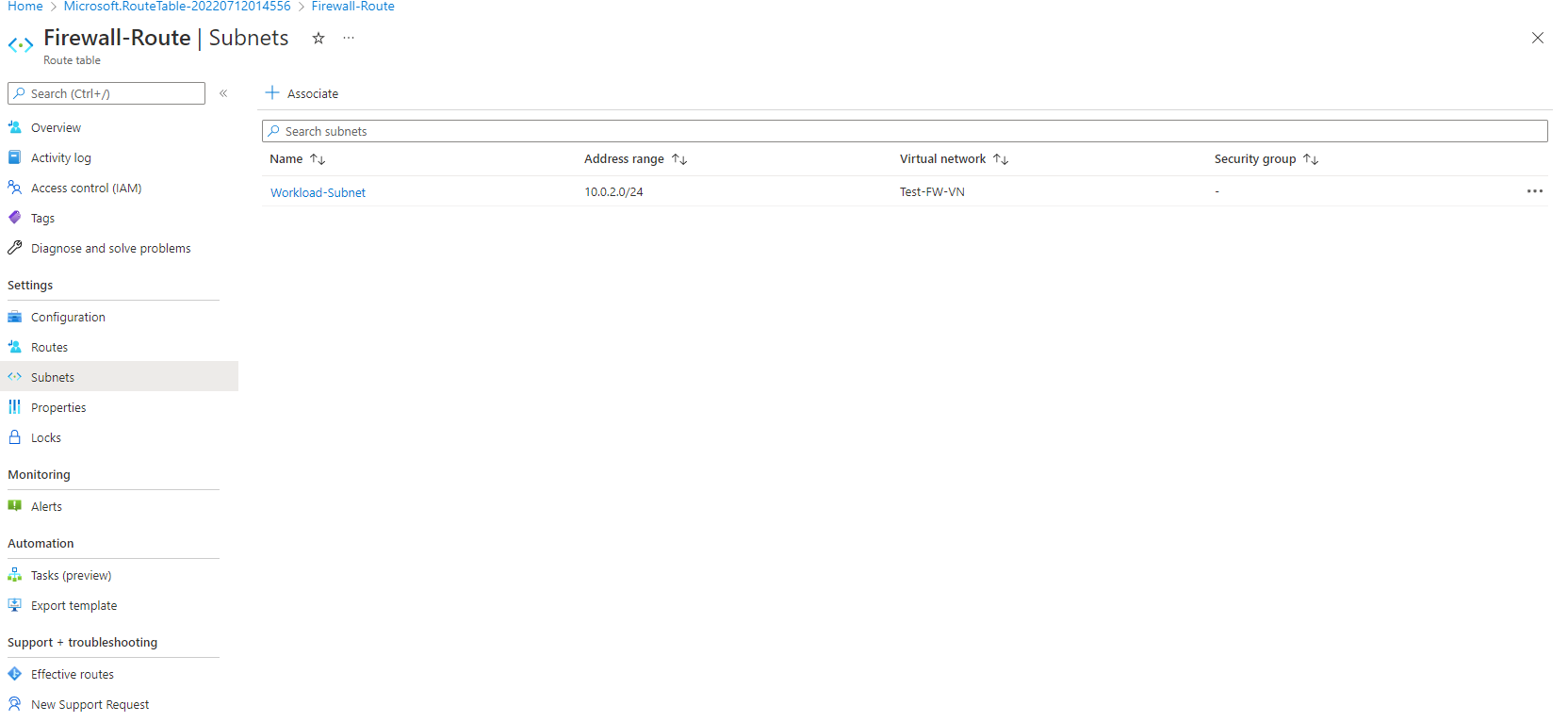
* Creating my Virtual network. I decided to use 10.0.0.0/16 for the IP range. I created the subnets that’s going to be used for the firewall and workload.



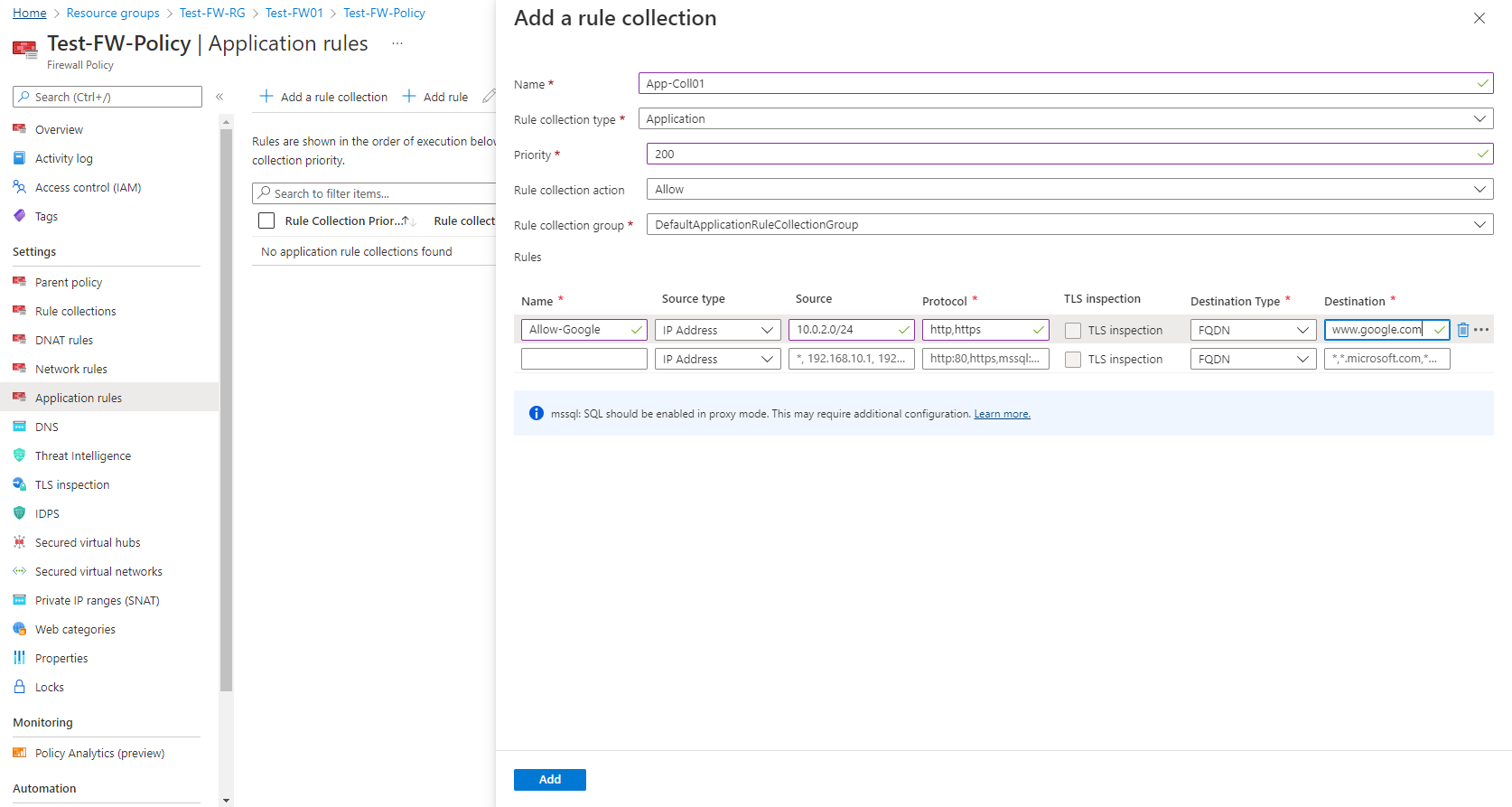
* Here I created and deployed my Firewall to the VNet.



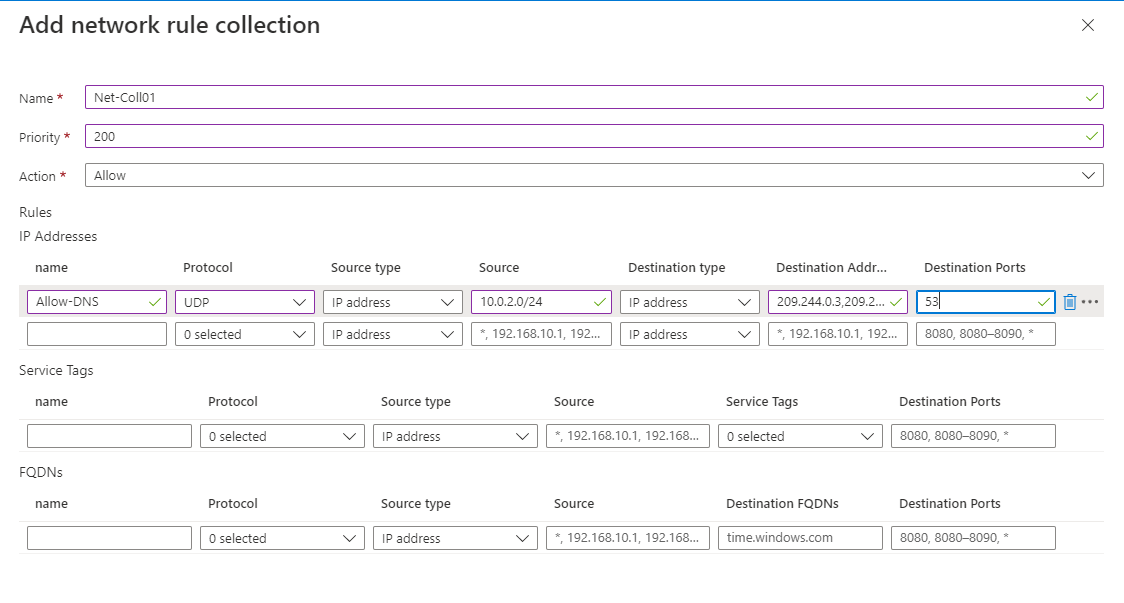
* Here I was creating a routing table that is going to hold the configured ACLs



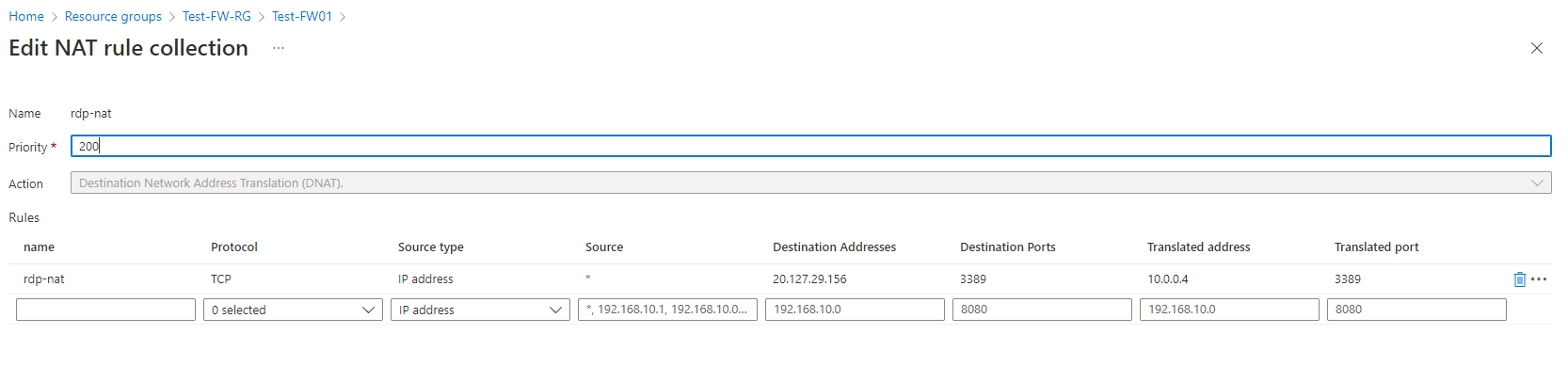
* Connected our Workload subnet to routing table.



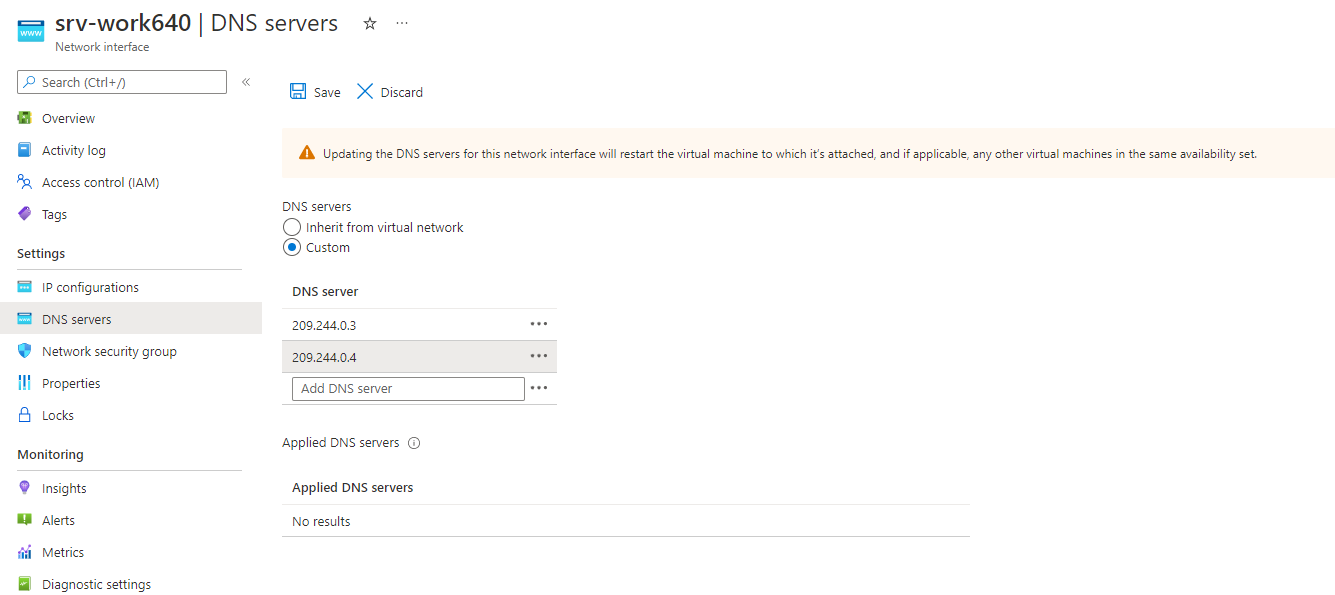
* Modifying our firewall policy to allow traffic going to Google.



* Created a Network Rule allowing outbound access to two IP addresses on Port 53 (DNS)



* Created a DNAT Rule which allows the remote desktop session to connect to the Srv-Work VM through the firewall



* Changing the Primary and Secondary DNS address for the Srv-Work interface.
* The final step is to test the firewall. Unfortunately, I’m using my work laptop and my organization has RDP blocked and won’t connect. But I only allowed access to google.com; Therefore, any other web pages attempts should be blocked unless I go back and configure the External DNS server.

Reminder: Once verifying everything has worked make sure you delete the resource group so you’re not being charged.

Resource

[Deploy & configure Azure Firewall using the Azure portal | Microsoft Docs](https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal)