Amanda Patterson

6/5/2021

Project 13 ReadMeFile

1. **Your network diagram –** See attached.
2. **A description of the deployment.**

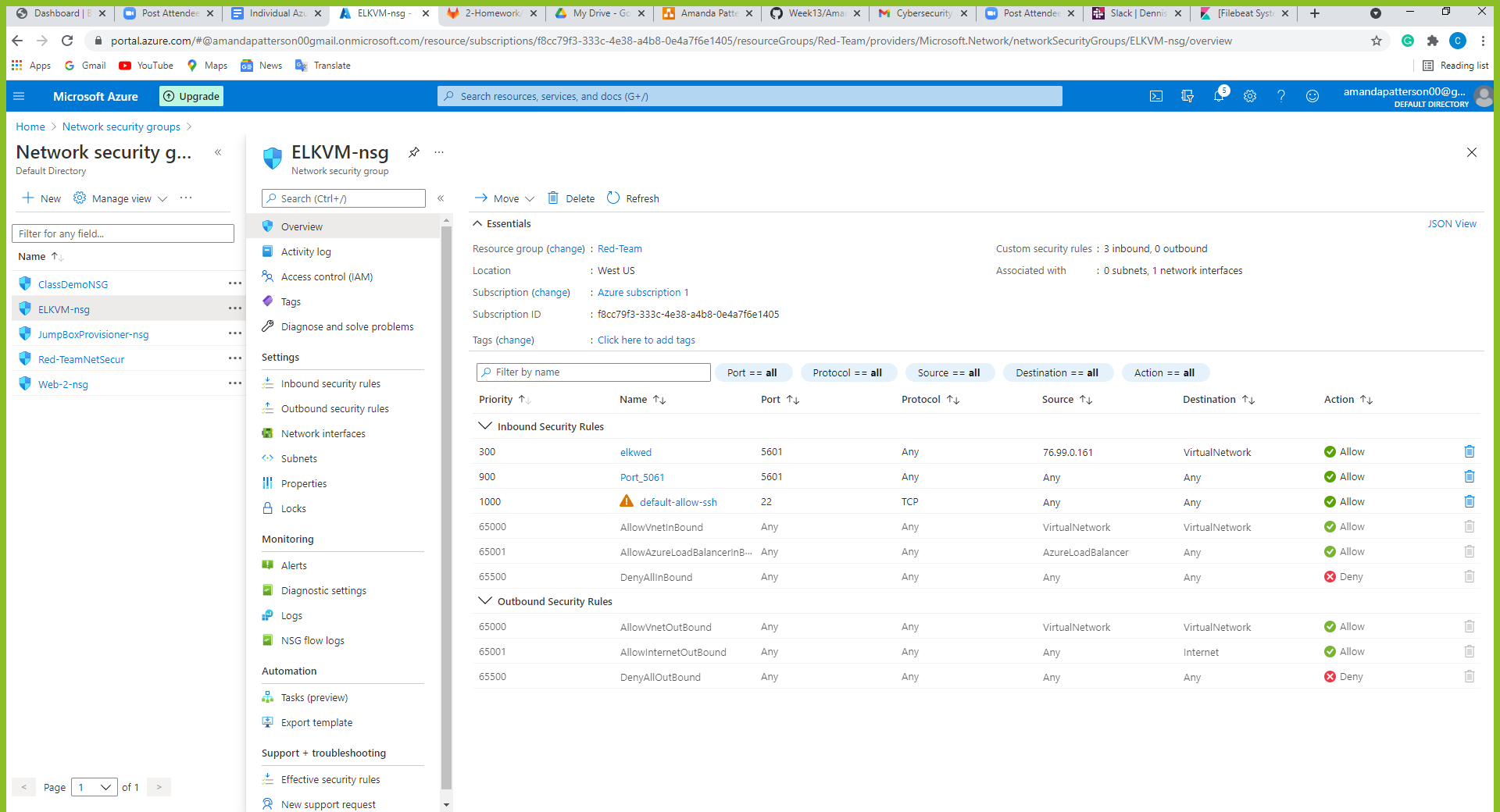
I configured an ELK stack server to set up a cloud monitoring system. To perform this task, I used Microsoft Azure cloud services and the Azure cloud portal.

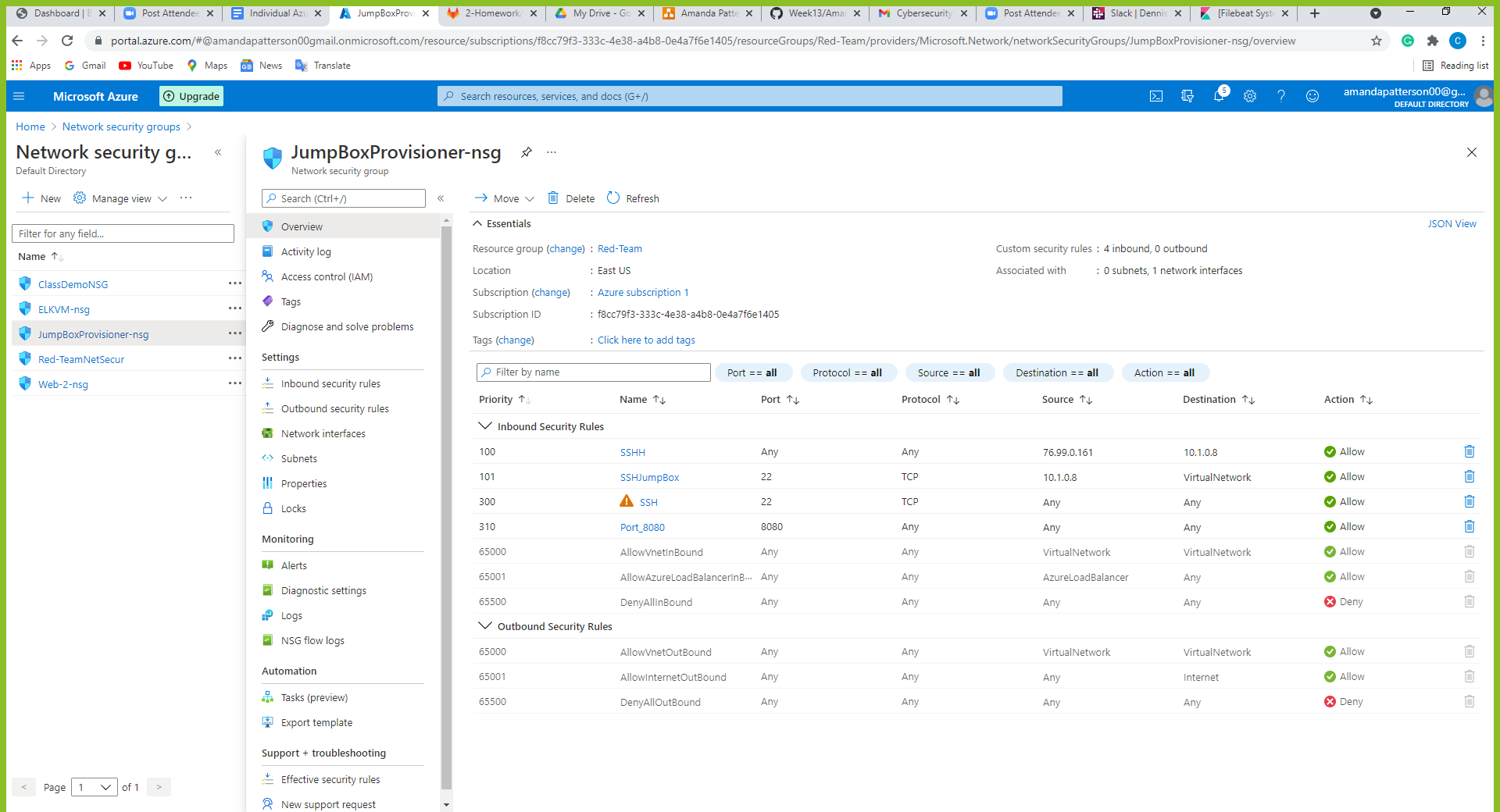
While using my personal using personal Azure accounts I set up my Resource Groups, Virtual Networks, Network Security Groups, and Virtual Machines.

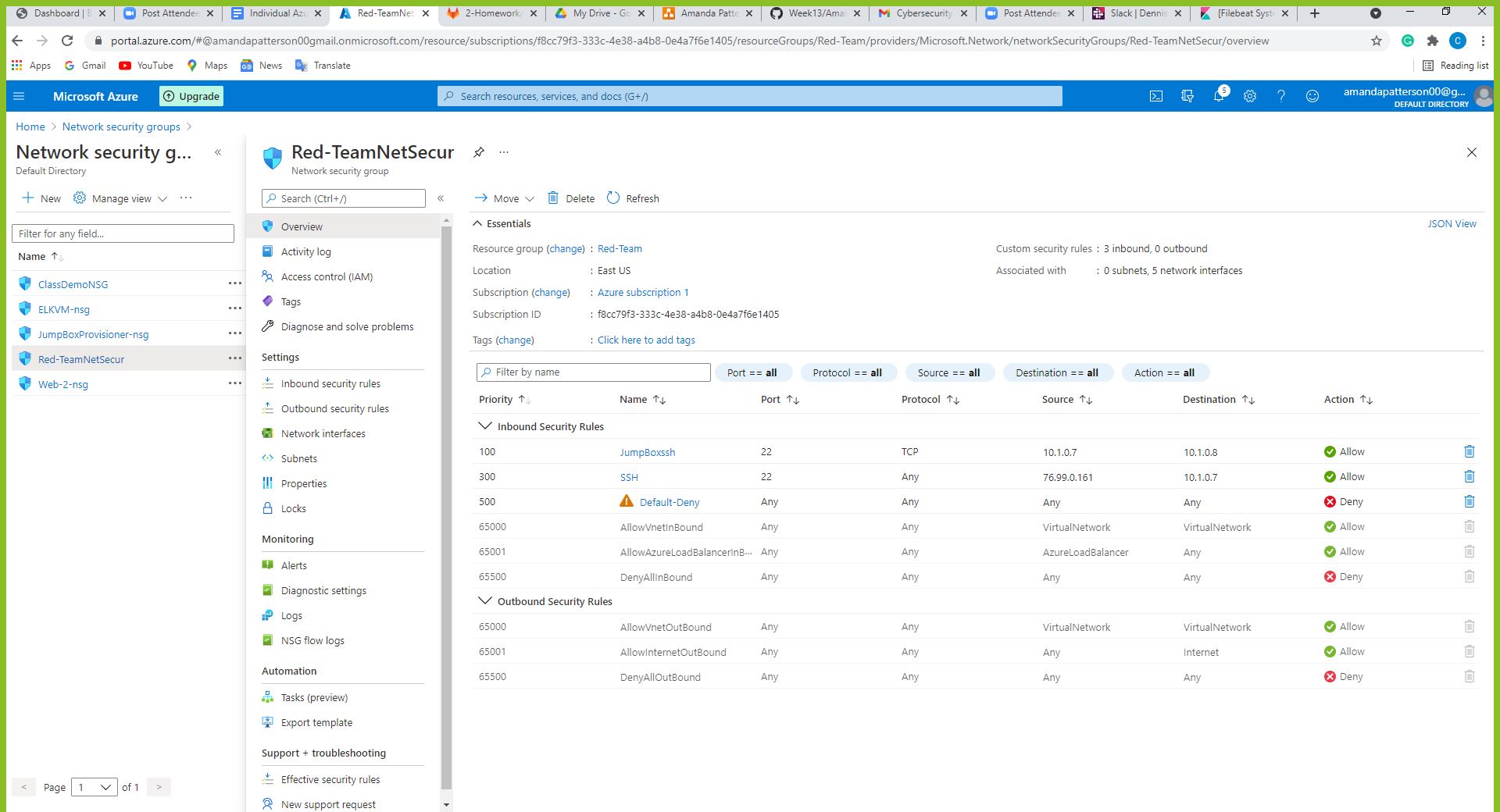
1. **Tables specifying access policies and network addresses.**

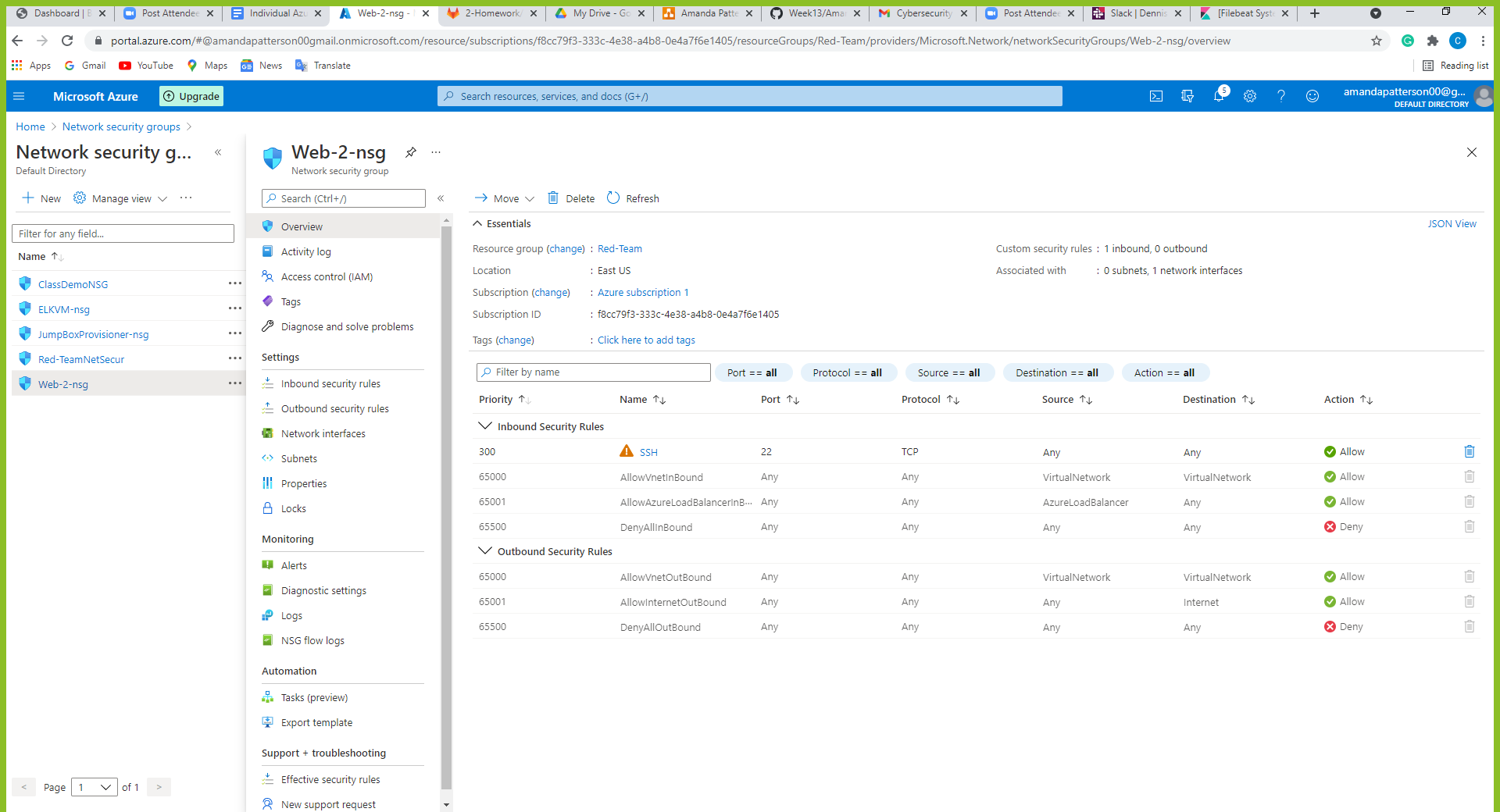
|  |  |  |
| --- | --- | --- |
| Virtual Networks | Elk-VNetWork | Red-TeamVNETWK |
| Address space | 10.2.0.0/16 | 10.1.0.0/16 |
| Location | West US | East US |

**Network Security Group Inbound/ Outbound Rules**









1. **A description of the investigation you completed using Kibana.**

The Kibaba part of the project highlighted identity and access management. I completed the task of creating an Ansible playbook which installed and configured an ELK container. I tested that the Ansible playbook could be ran on my new VM. I also verified the VM was running on the Elk container. My final step was to restrict access to the ELK VM using Azure's network security groups (NSGs). I add my public IP address to a whitelist and set up network security group inbound rules that would allow the ELK stack's web server runs on port 5601. I continued building up my ELK server by installing Filebeat.

We learned that Filebeat helps generate and organize log files to send to Logstash and Elasticsearch. Specifically, it logs information about the file system, including which files have changed and when. We also learned that Filebeat is often used to collect log files from very specific files, such as logs generated by Apache, Microsoft Azure tools, the Nginx web server, or MySQL databases.

1. **Usage instructions.**

For this project I monitored the Apache server and MySQL database logs generated by DVWA. Filebeat was installed on the DVWA container I created during the cloud security week. This allowed a source of logs after I complete my deployment. After the installation. I verified that Kibaba was able to test incoming data. This was successful.