Project:
Securing the Perimeter

Directions and Submission Template

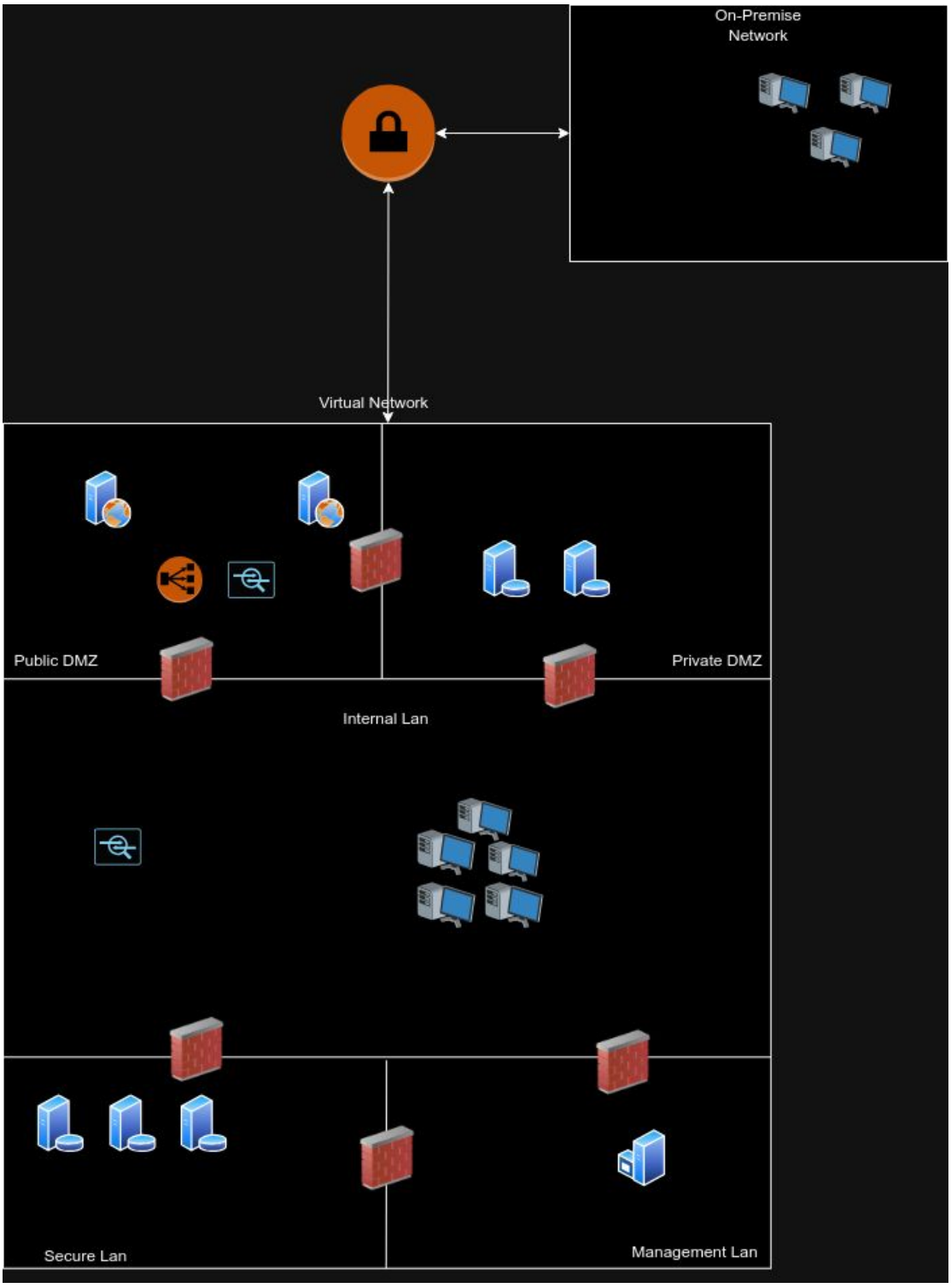
Mohamad Abdelnaby

2024/04/18

Section 1

Designing a Secure Network Architecture

1.1 Designing the Network

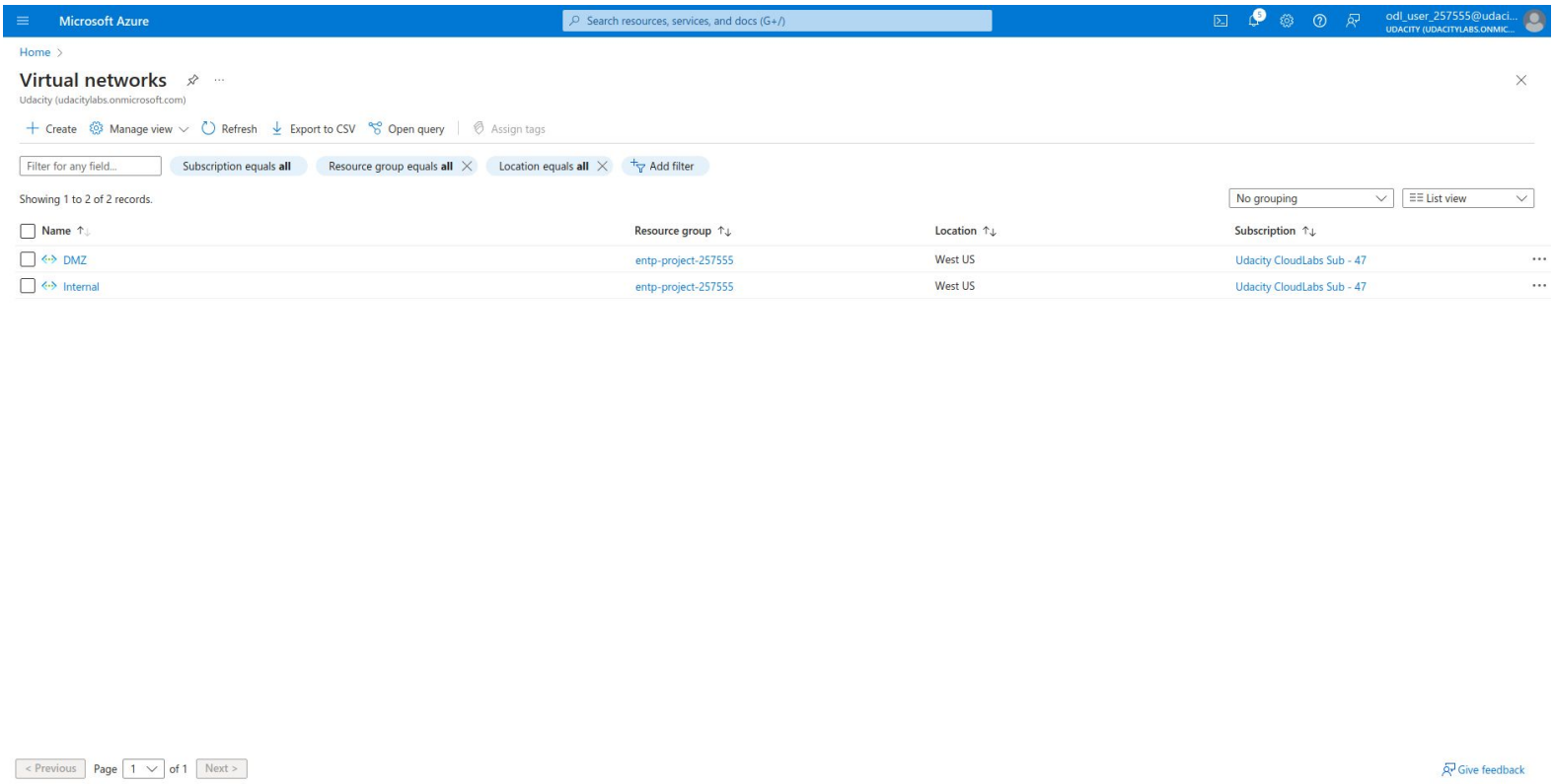


Section 2

Building a Secure Network Architecture in Azure

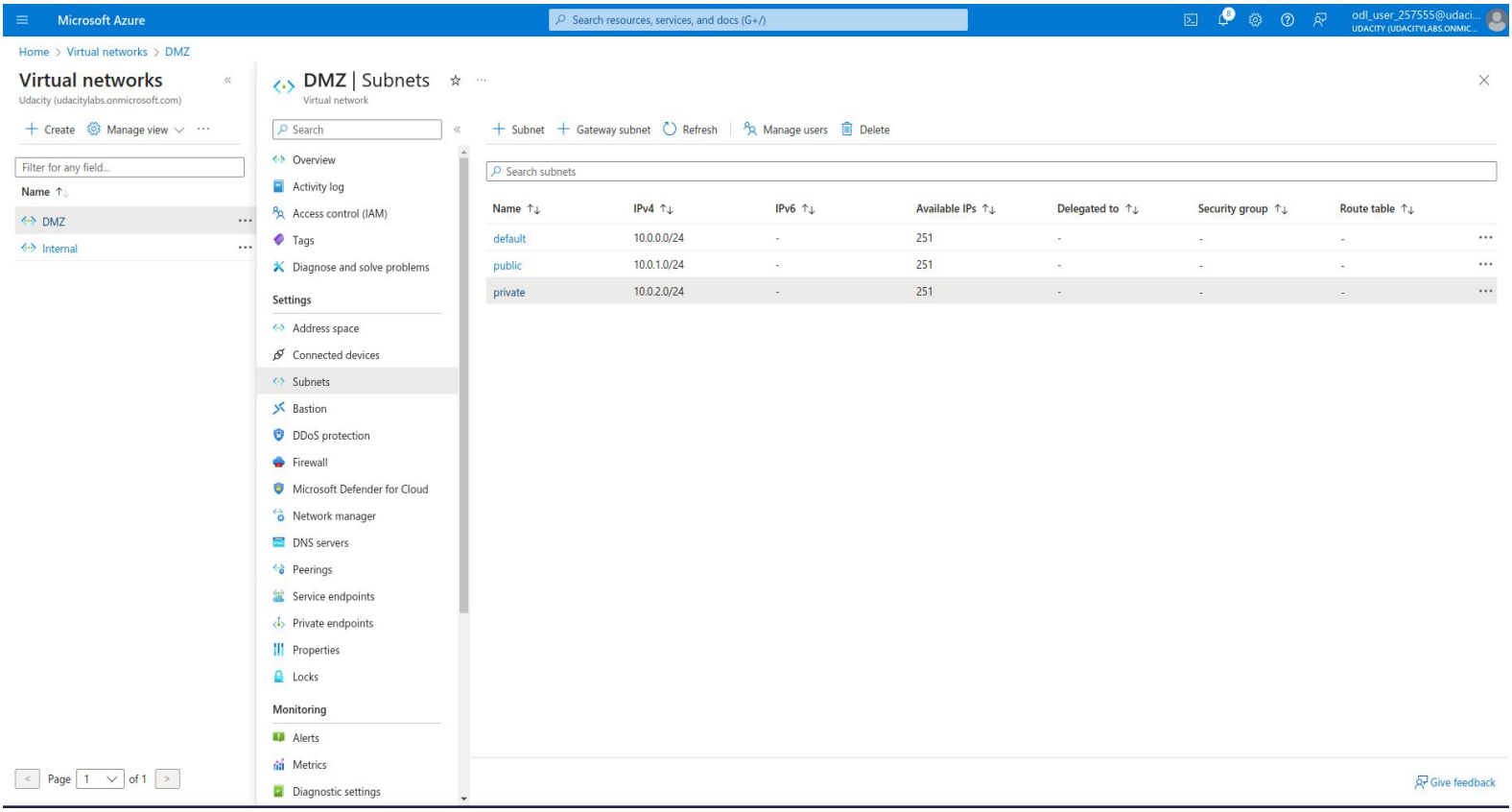
2.1.1 Screenshot

Create two Azure Virtual Networks in the resource group ‘entp-project’. Label one for your DMZ and one as your Internal.



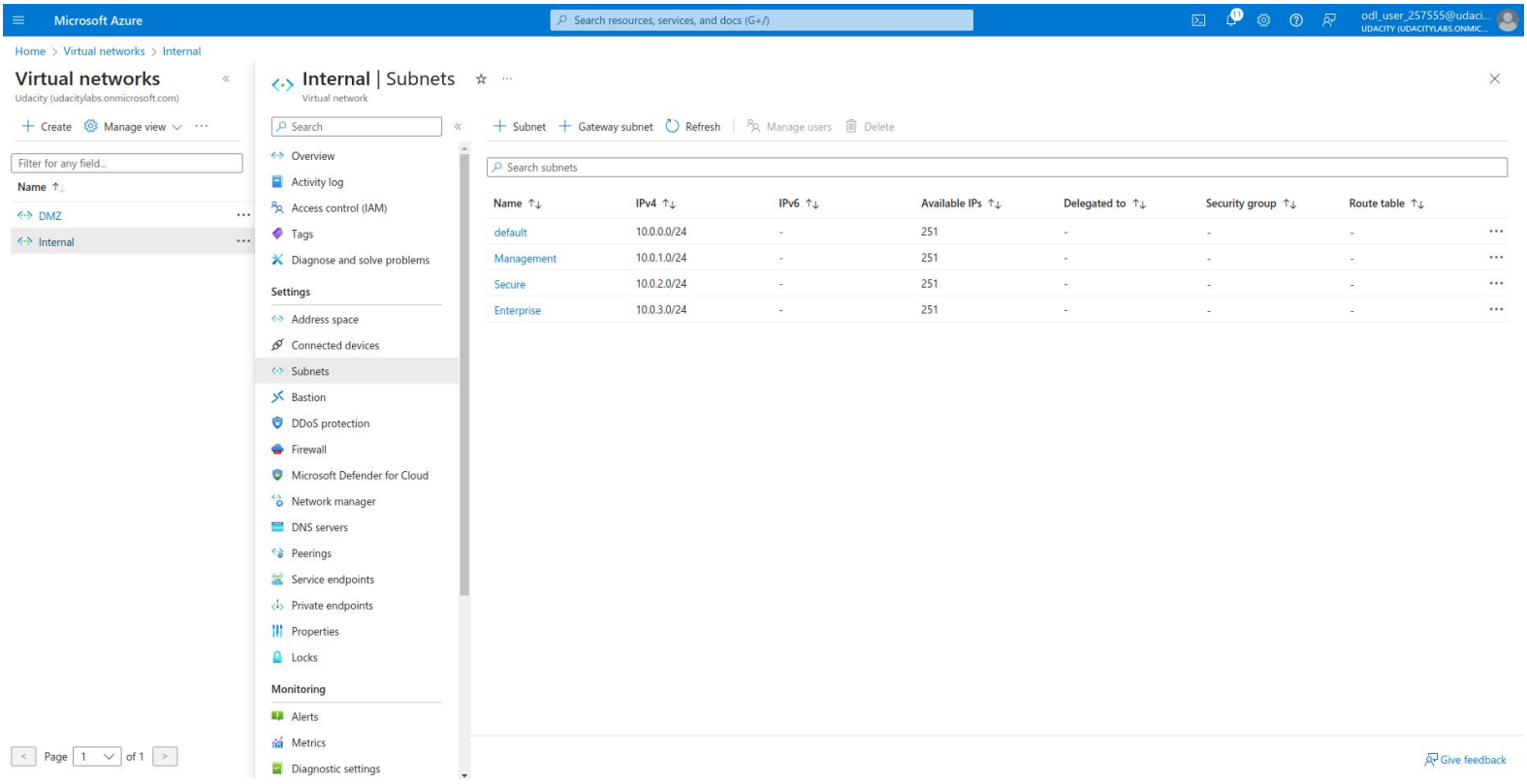
2.1.2 Screenshot

Create 2 subnets within your DMZ - subnets should be public and private.



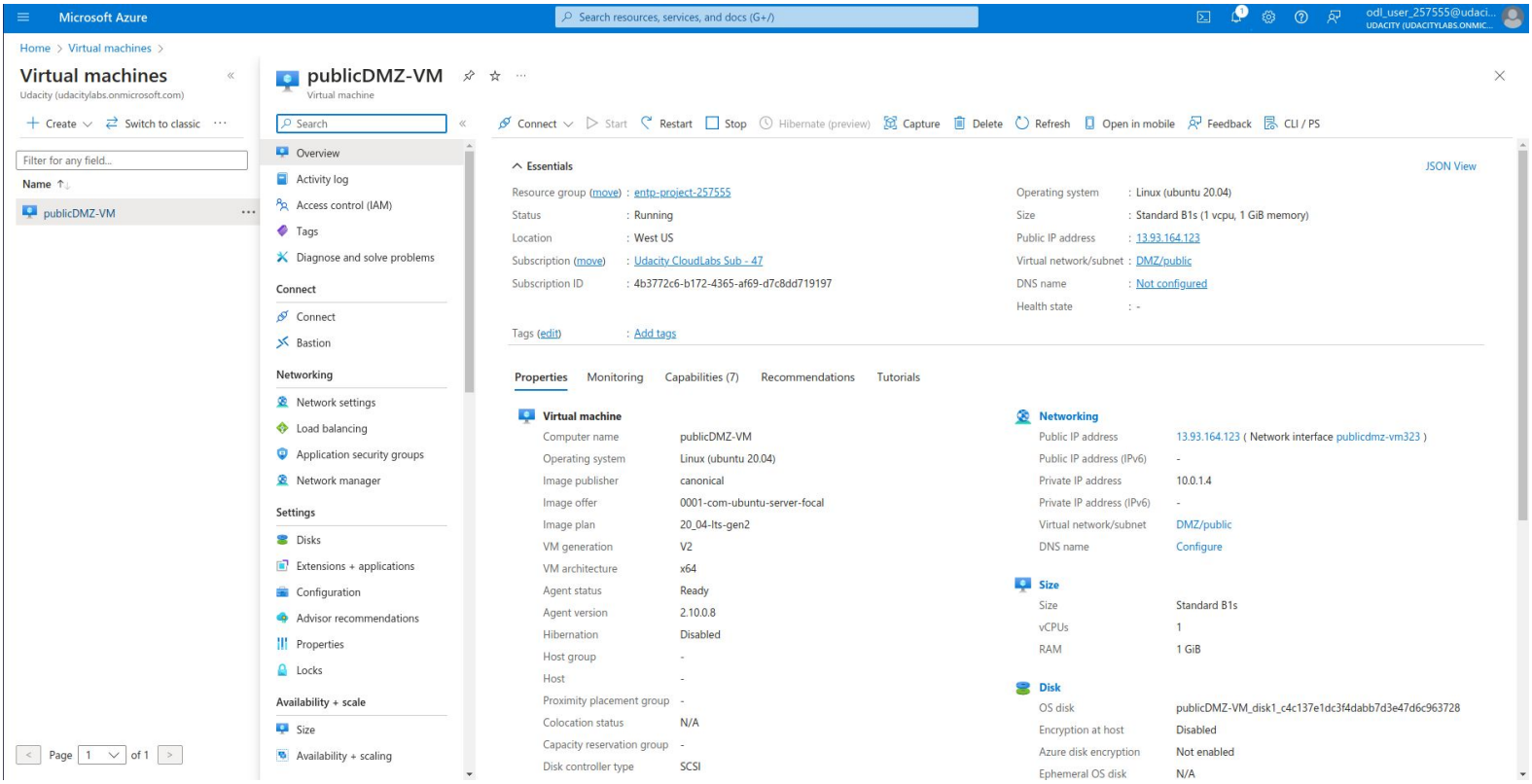
2.1.3 Screenshot

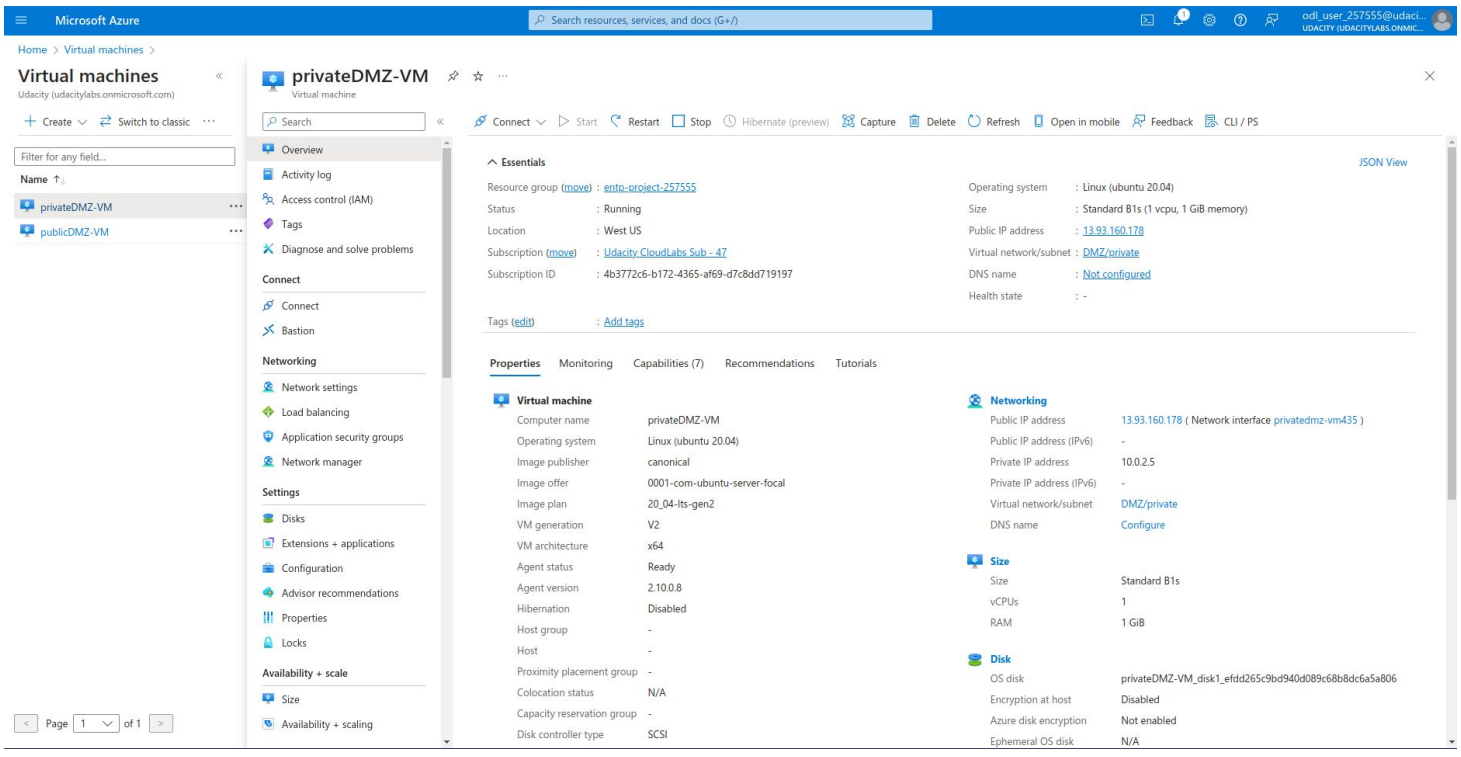
Create three subnets in your internal network and label them Management, Secure, and Enterprise.



2.2.1 Screenshot

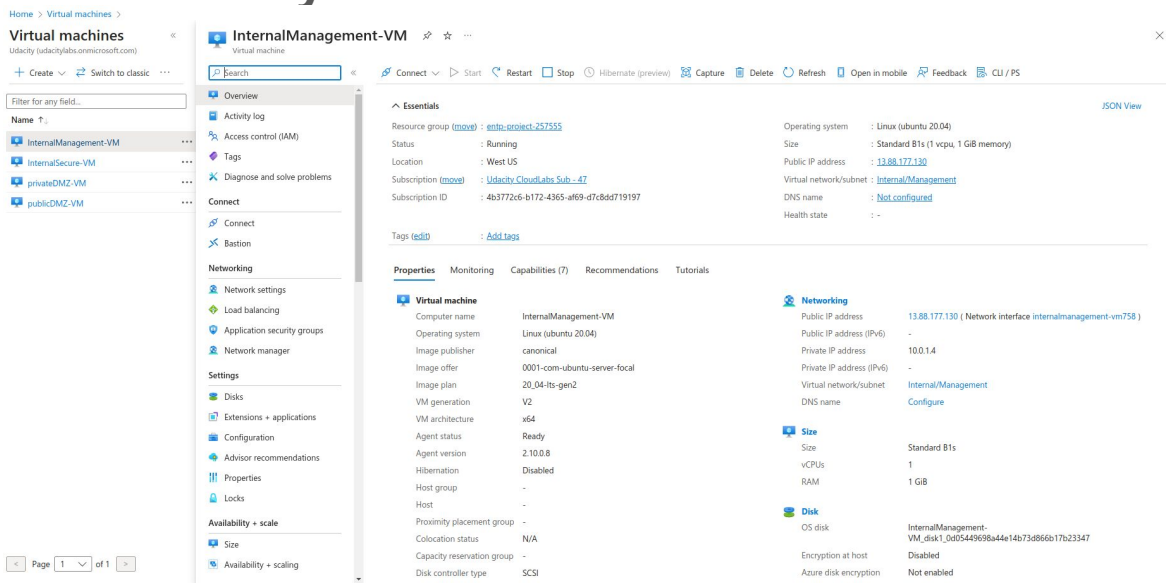
Create one VM in each of your public and private DMZ subnets. Please only use Standard_B1s for your VM size and select the Linux Ubuntu 18.04 image, otherwise you will encounter an error.

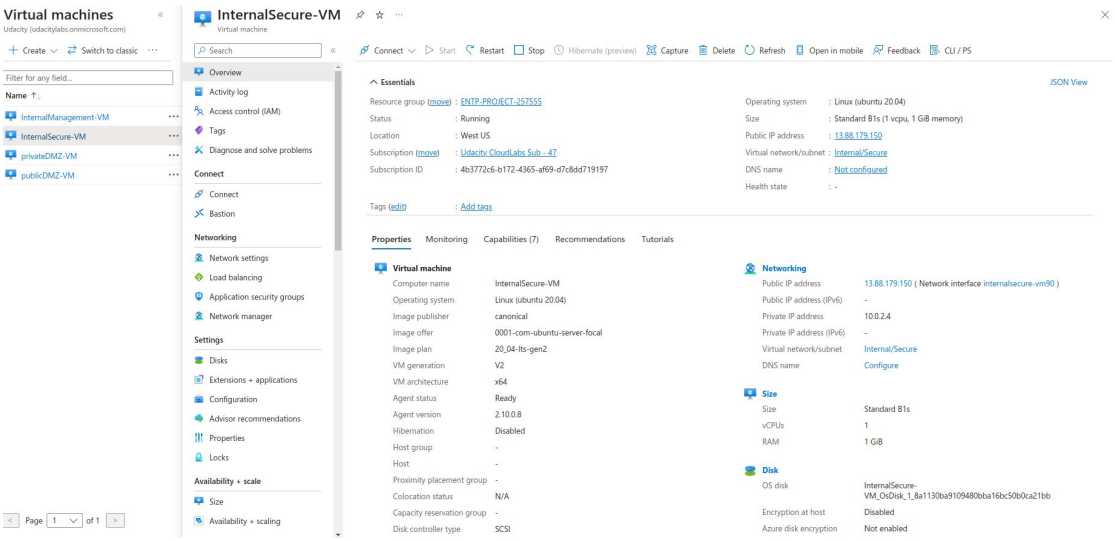


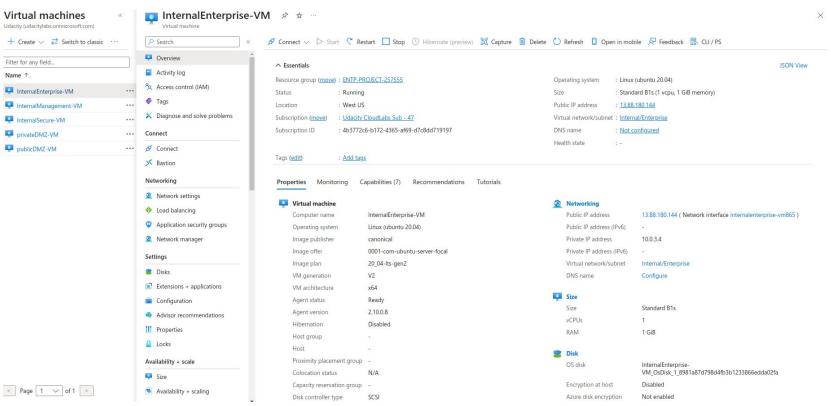


2.2.2 Screenshot

Create one VM in each of your Management, Secure, and Enterprise internal subnets. Please only use Standard_B1s for your VM size and select the Linux Ubuntu 18.04 image, otherwise you will encounter an error.

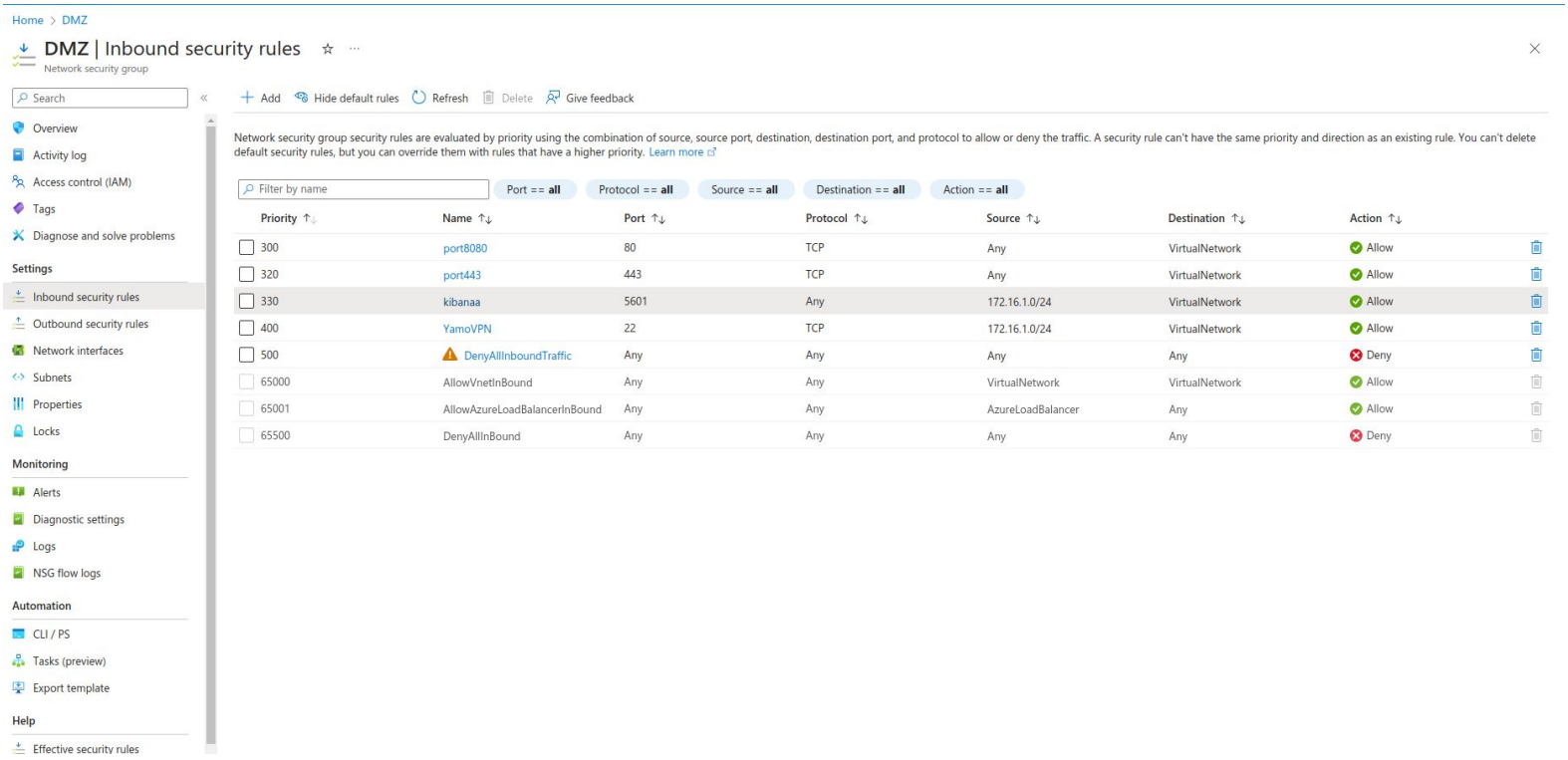






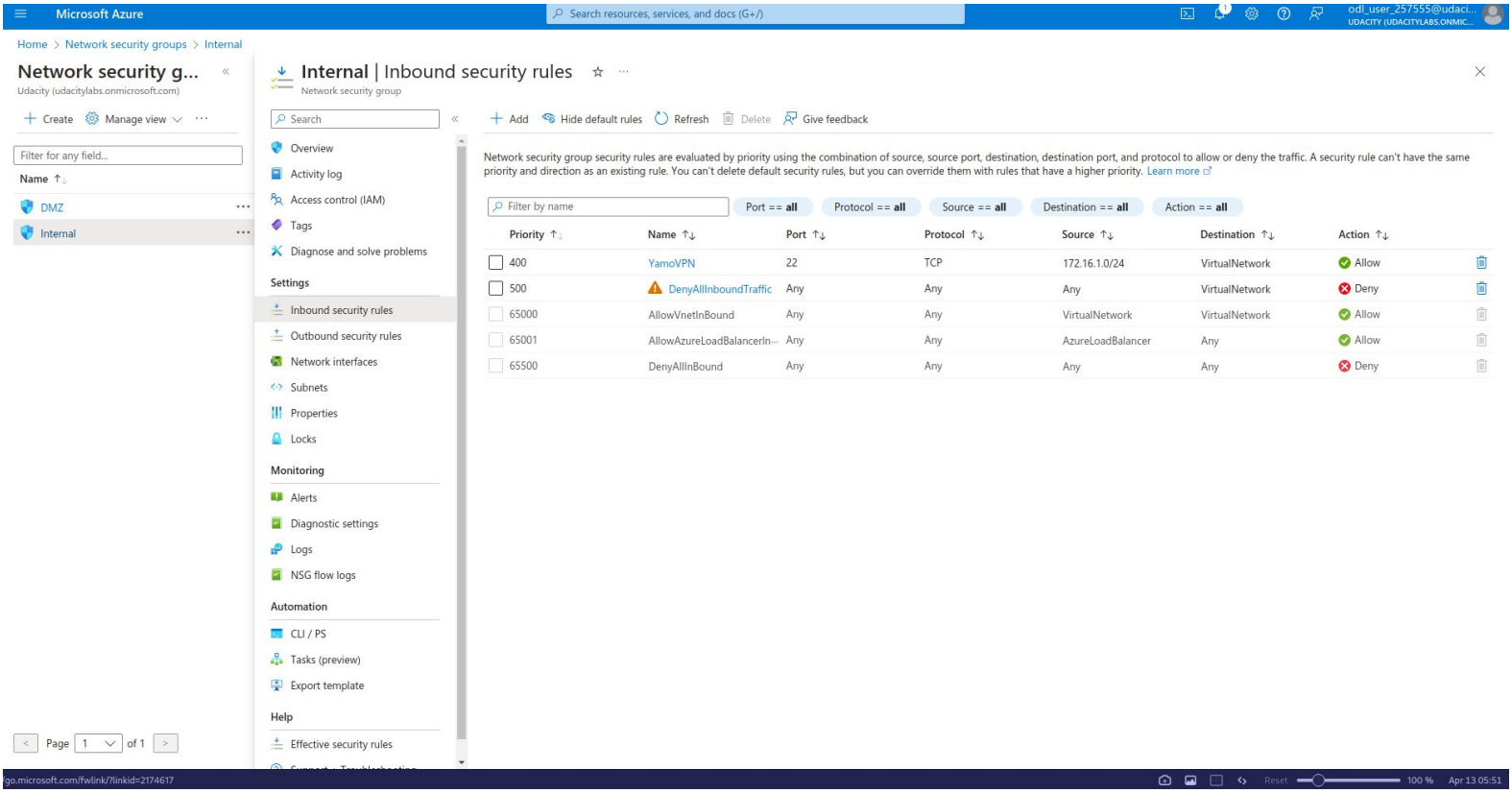
2.3.1 Screenshot

Traffic rules in your DMZ.



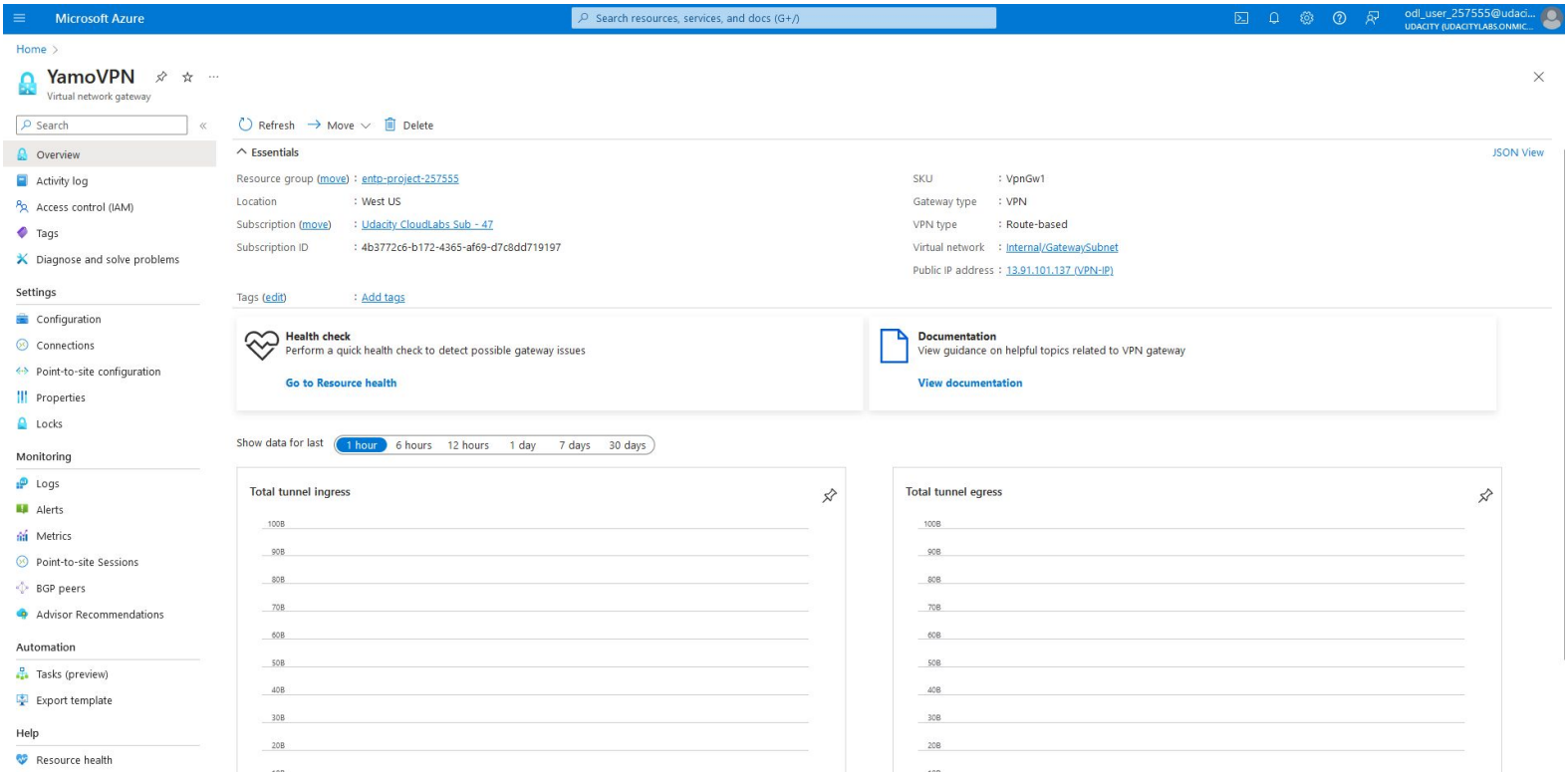
2.3.2 Screenshot

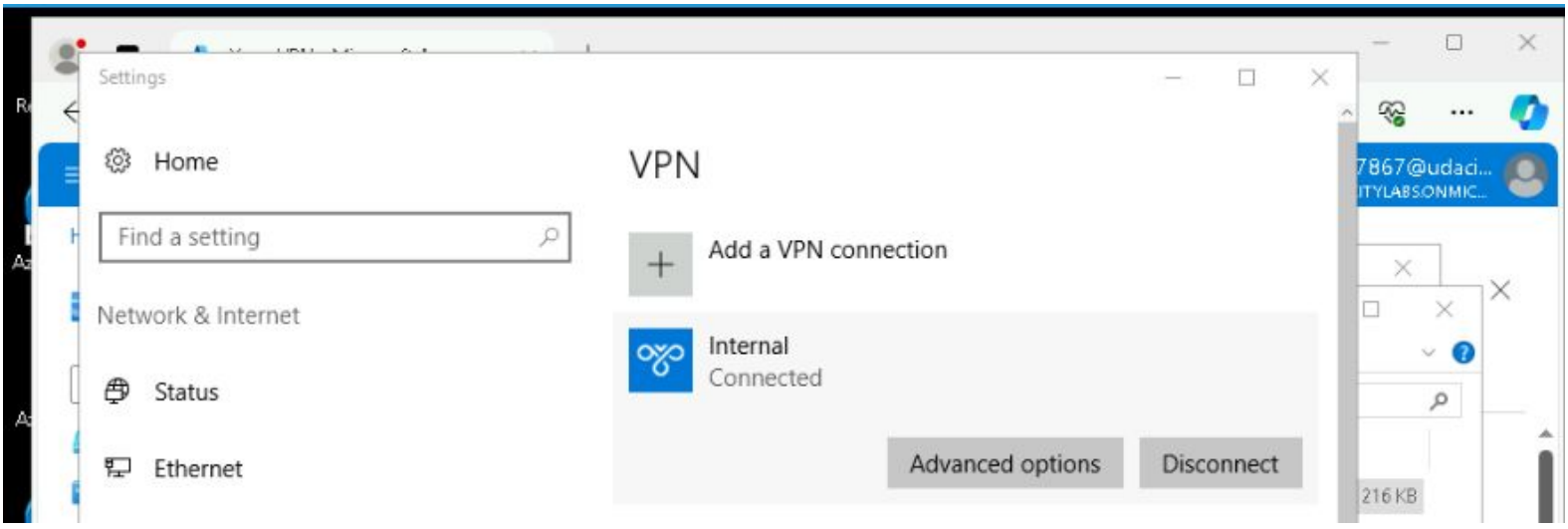
Traffic rules in your Internal network.



2.4.1 Screenshot

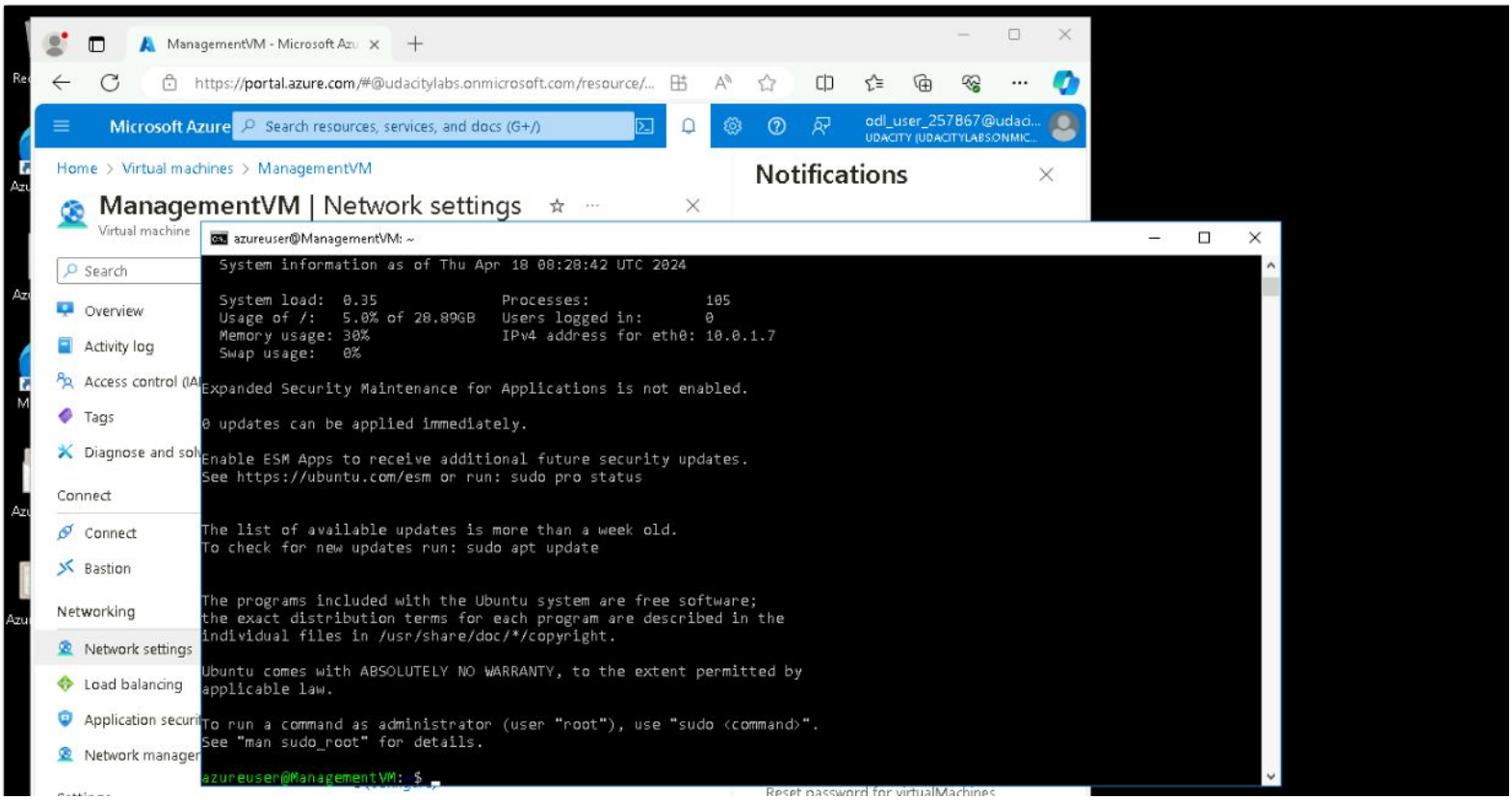
Create a VPN to connect to your internal network.





2.4.2 Screenshot

Test VPN connection by connecting to one of the VMs in your internal network.

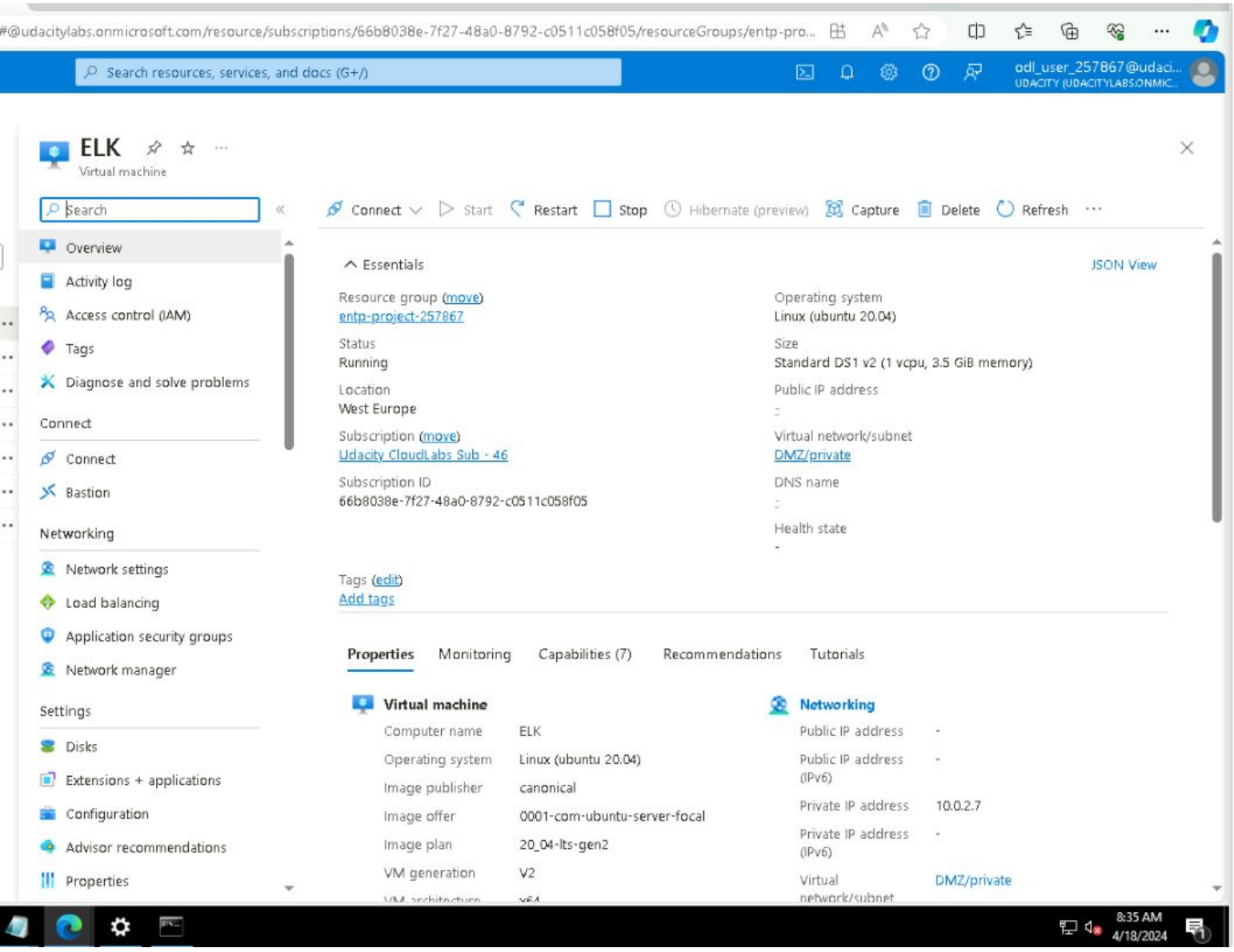


Section 3

Continuous Monitoring with a SIEM

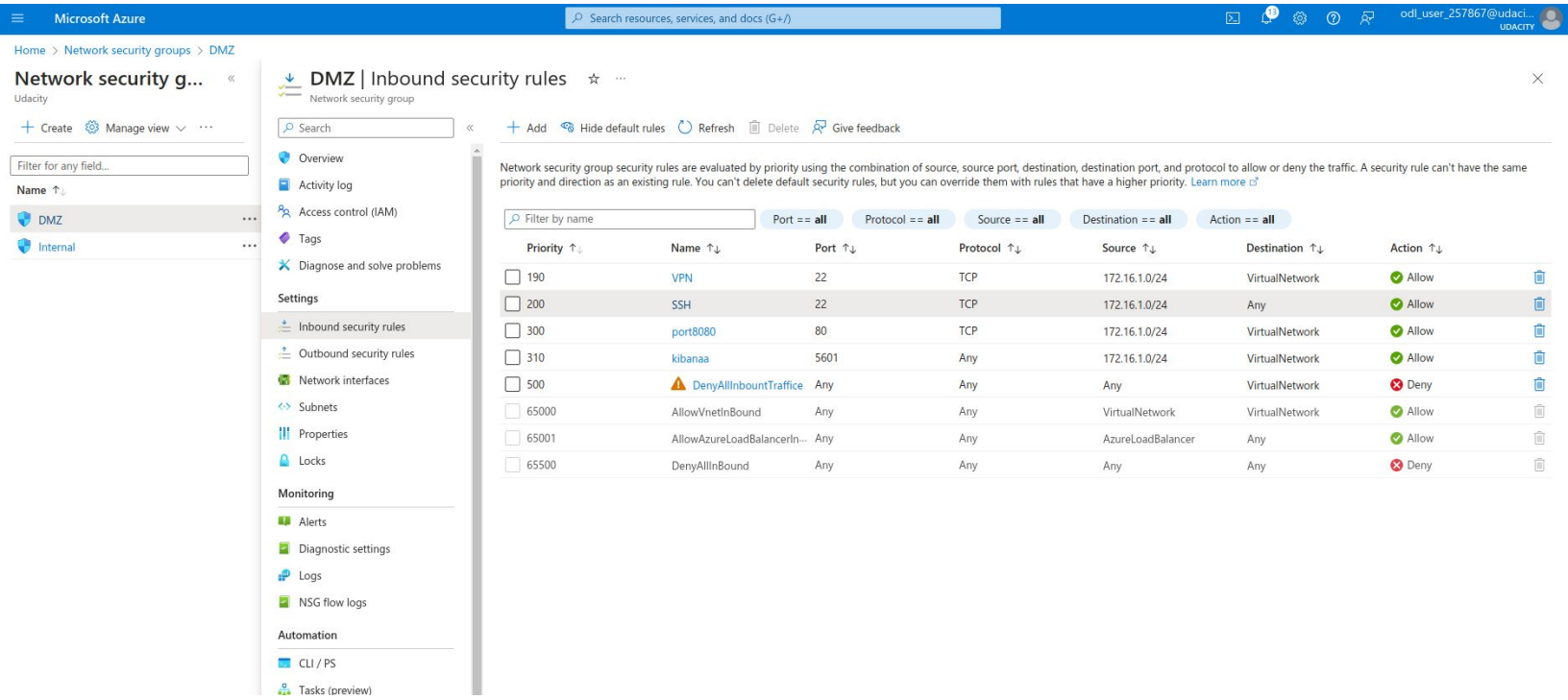
3.1.1 Screenshot

Create a VM in your private DMZ. On that VM, go through the process to create an ELK Server. For your Elk Server use the VM size DS1_v2 and Linux Ubuntu 18.04 image.



3.1.2 Screenshot

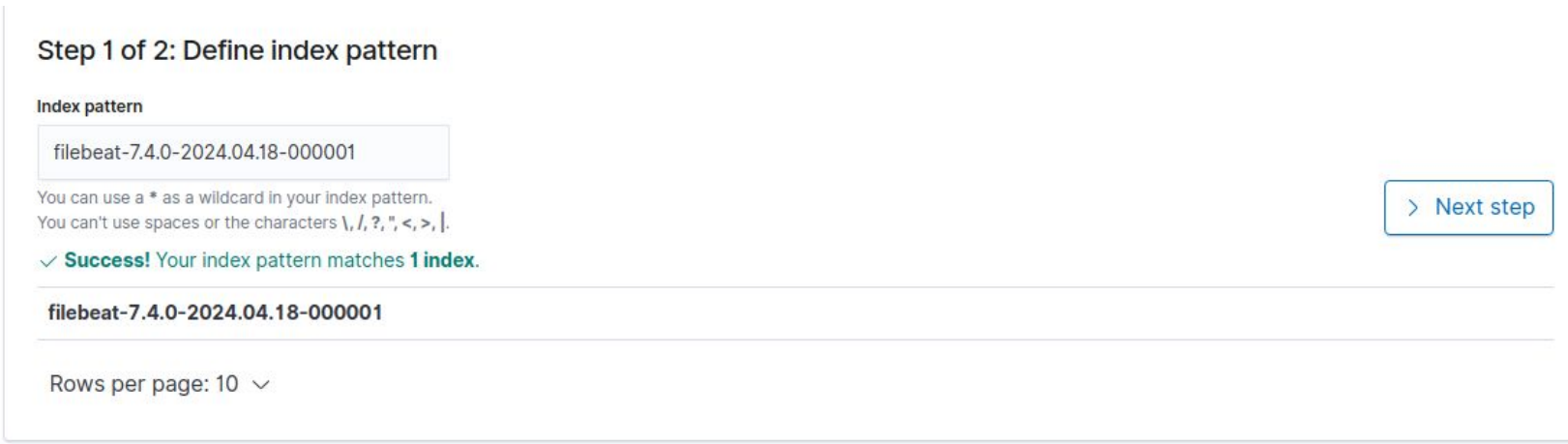
Set up routing to only allow traffic inbound to the server from both your virtual networks, and make sure Kibana is only accessible when you're on the network.



3.2.1 Screenshot

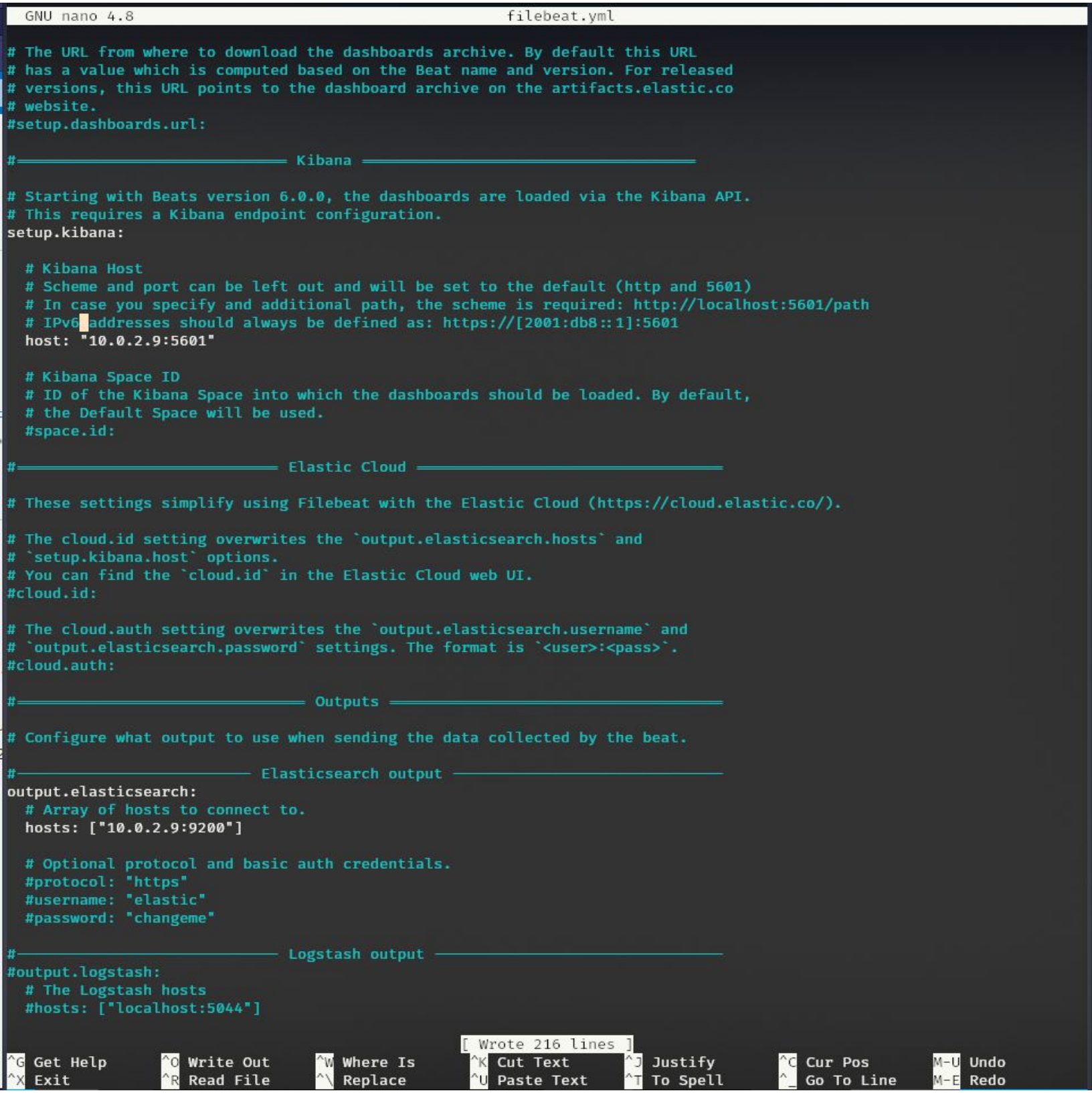
Install Filebeat on your web servers and show the Filebeat service as active.

```
azureuser@WebServerVM:/etc/filebeat$ sudo filebeat modules enable system
Enabled system
azureuser@WebServerVM:/etc/filebeat$ sudo filebeat modules enable apache
Enabled apache
azureuser@WebServerVM:/etc/filebeat$ sudo filebeat setup
Exiting: Couldn't connect to any of the configured Elasticsearch hosts. Errors: [Error connection to Elasticsearch http
://10.0.2.9:9200: Get http://10.0.2.9:9200: dial tcp 10.0.2.9:9200: i/o timeout]
azureuser@WebServerVM:/etc/filebeat$ sudo filebeat setup
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded machine learning job configurations
Loaded Ingest pipelines
azureuser@WebServerVM:/etc/filebeat$ sudo service filebeat start
azureuser@WebServerVM:/etc/filebeat$
```



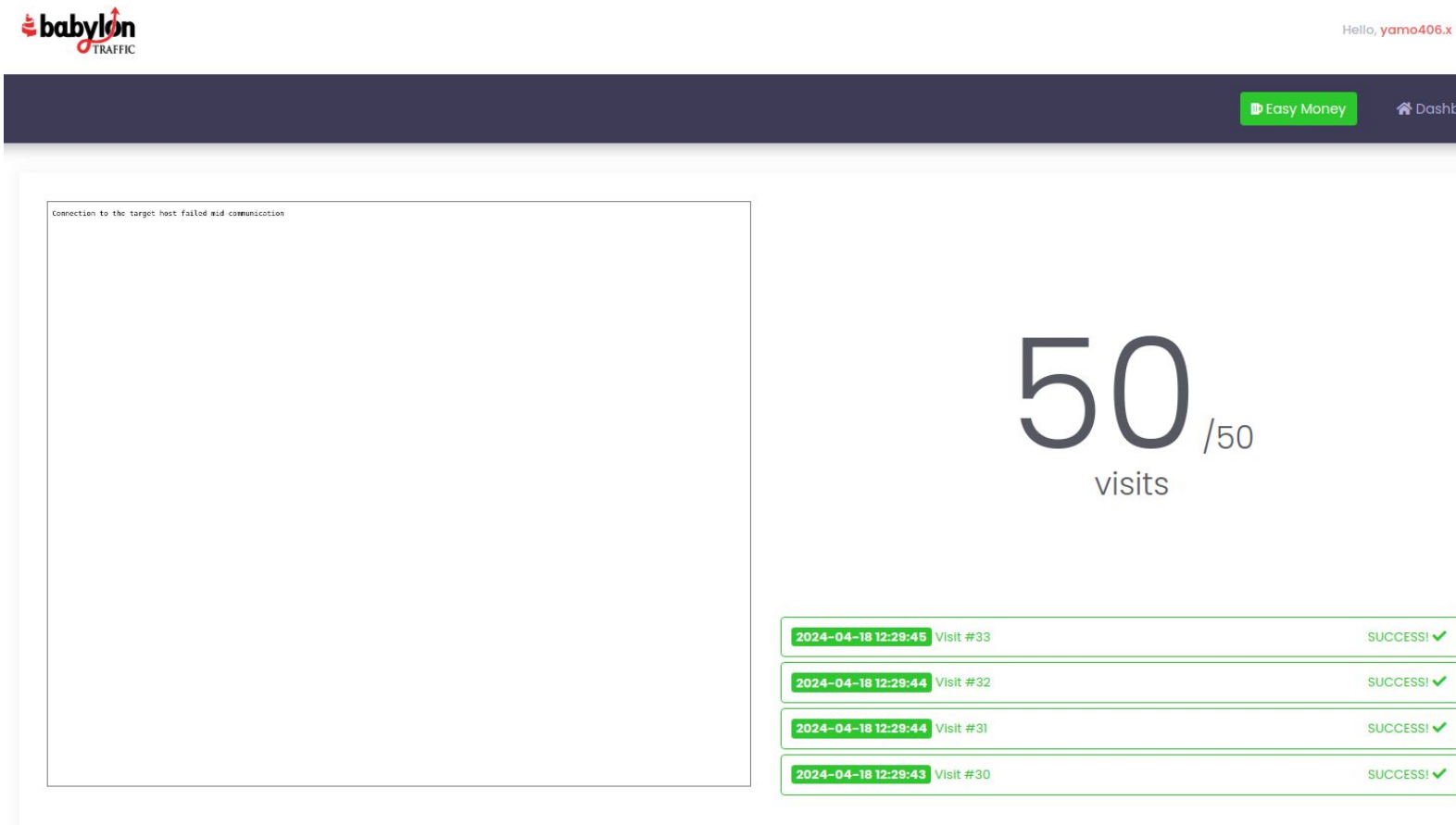
3.2.2 Screenshot

Configure Filebeat to route web server logs to Elasticsearch.



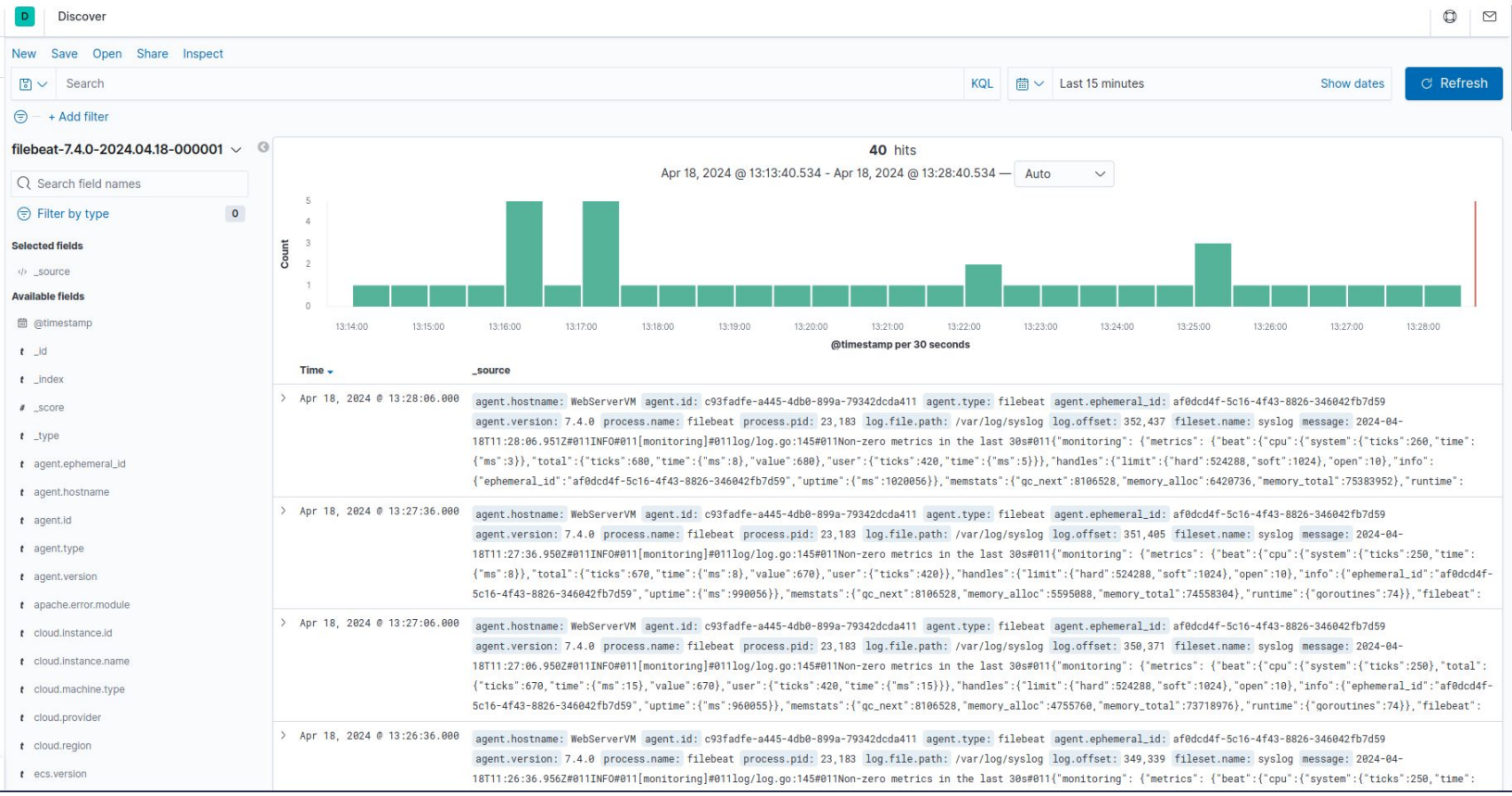
3.2.3 Screenshot

Simulate web traffic to your web servers using https://www.babylontraffic.com.



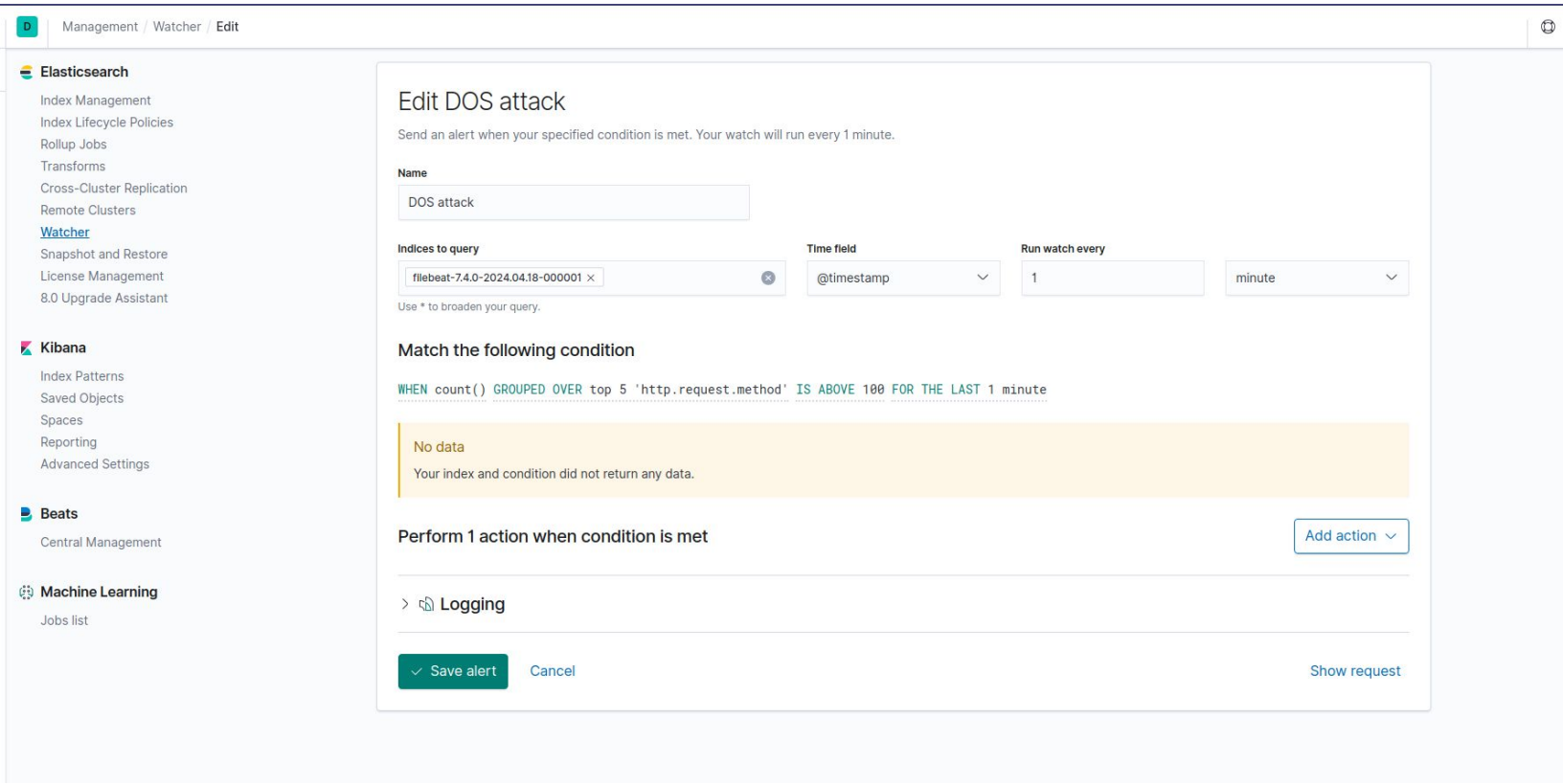
3.2.4 Screenshot

Web server logs appear in Kibana.



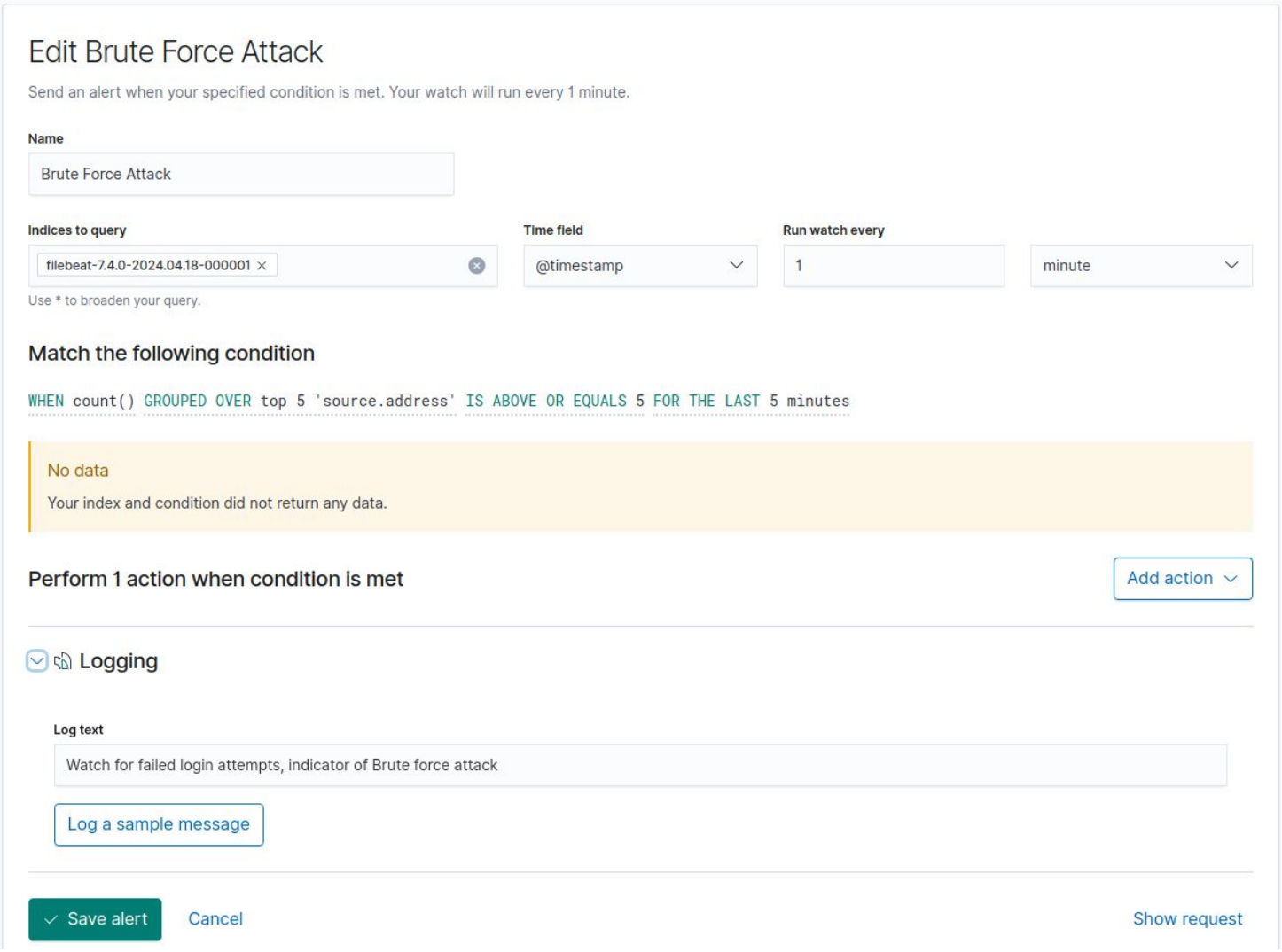
3.3.1 Screenshot

Create an alert for DoS attack.



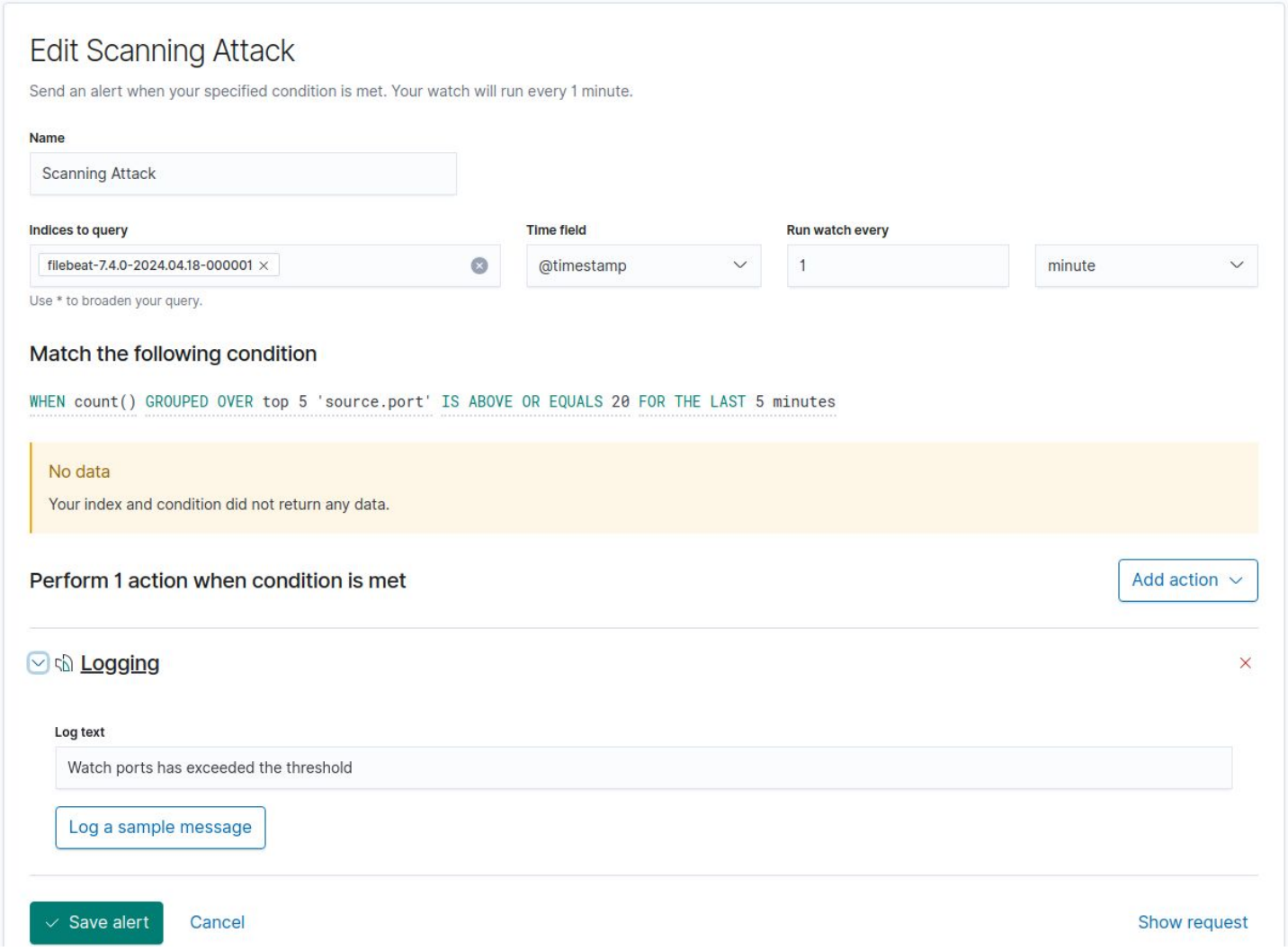
3.3.2 Screenshot

Create an alert for Brute Force attack.



3.3.3 Screenshot

Create an alert for a scanning attack. During the scan, an attacker is looking to identify what ports are open.



DOS Attack Playbook

Preparation:

- Train the Security employees on identifying the true DOS attack alerts from false positives.
- All the employees have a direct contact to the security lead in case of DOS attack

Detection & Analysis:

- Set up alerts for detecting DOS attacks, have them check if they get multiple requests that could threaten to flood the server and shutdown
- Document the logs including the DOS attack alert
- Prioritize business continuity if an attack will cause operations to stop immediately document the Source IP of the attack.

Containment, Eradication & Recovery:

- Block the Source IP responsible for the attack
- Get all the threat actor details from the logs and document it
- If any service goes down restart and get it up and running, small patches for business continuity

Post-incident Activity:

- Document the incident details, the threat actors information
- Can we do anything extra to mitigate future DOS attacks?
- Hold a meeting to discuss the incident.

Brute Force Attack Playbook

Preparation:

- Train the Security analysts on identifying a Brute force attack
- Contact information of a security lead who can answer at the time of incident, multiple tech leads with separate shifts covering the full 24/7

Detection & Analysis:

- Check for alerts of failed logins from the same IP for a username.
- Check for alerts of different login geolocation for a username.
- Analyze the logs in out of hours logins.

Containment, Eradication & Recovery:

- Block the IP address if it's not a trusted IP of an employee, lock the account.
- Did the threat actor get into the network? (Y/N)
    - Y: Determine the damage done i.e. infiltrated machines and isolate the machine from the network and block the IP
    - N: Block the IP and monitor the next hour for other similar attacks from other IPs

Post-incident Activity:

- Document incident details
- Document threat actor information from the logs and add him to the blocked list of unauthorized IPs
- Hold a meeting to discuss the incident.
- Can we improve something to prevent future similar incidents?

Scanning Attack Playbook

Preparation:

- Train employees on identifying a scan attack on the ports of the machine or server on the network.
- Available access to a security lead 24/7
- Close all unused ports, use firewalls, and use DMARK for email authentication.

Detection & Analysis:

- Monitor for alert of a scan of ports on the network

Containment, Eradication & Recovery:

- Block the IP scanning and monitor next hour for similar attacks
- Did the threat actor gain access to the network? (Y/N)
    - Y: isolate the infected machines, and block the IP
    - N: Block the IP and monitor for similar attacks

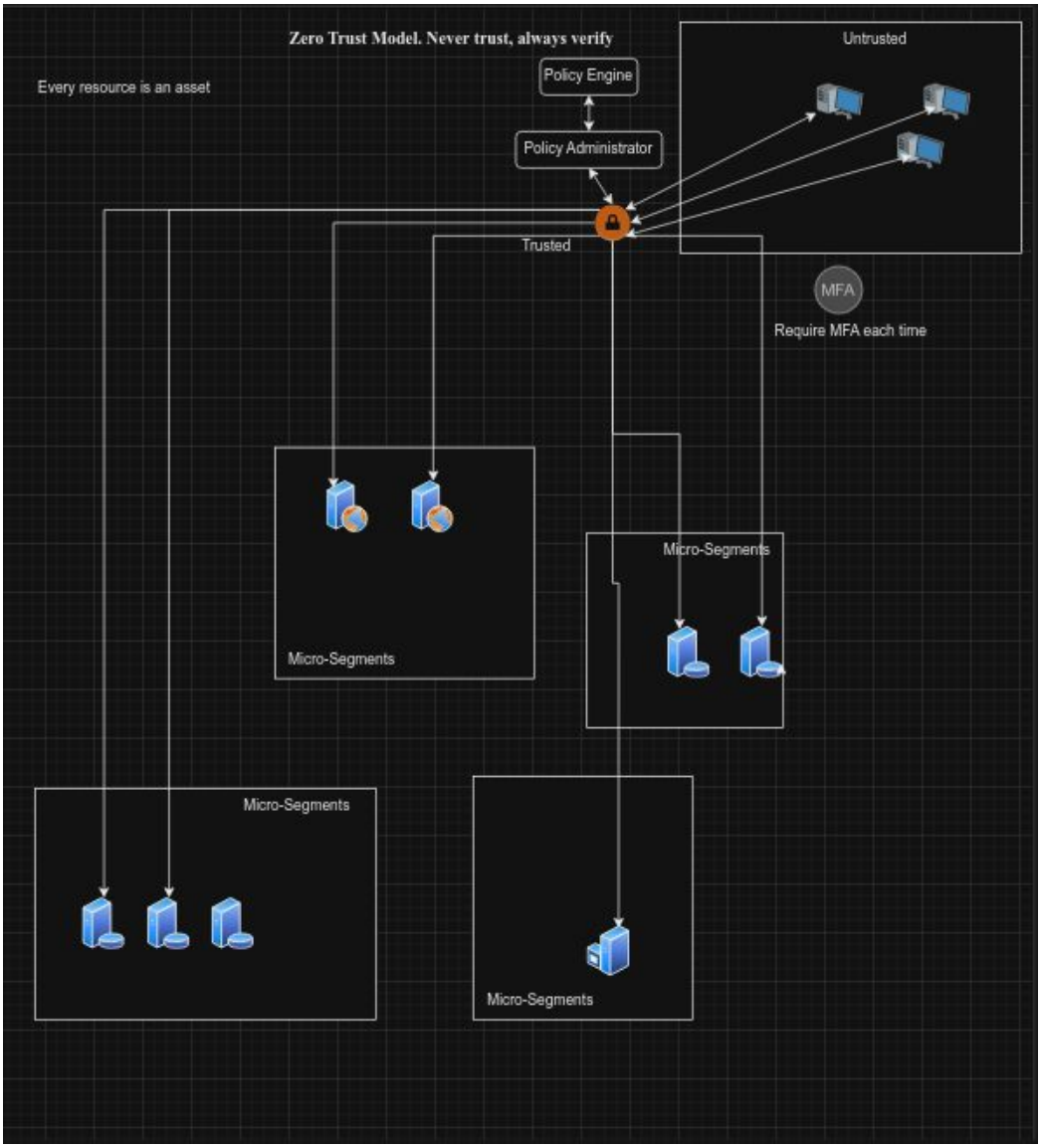
Post-incident Activity:

- Hold a meeting to discuss incident details
- Can we improve anything to prevent future attacks?
- Log incident details and threat actor information.

Section 4

Designing a Zero Trust Model

4.1 Zero Trust Model



4.2 Modern Architecture vs. Zero Trust

	Zero Trust	Secure Network
Core Philosophy	Assumes no trust within the network. Every user and device, regardless of origin (internal or external), must be continuously authenticated and authorized before granting access to resources.	Relies on a perimeter-based approach. It establishes strong security controls around the network's edge (firewalls, intrusion detection systems) to create a trusted internal zone. Once inside, users and devices generally have more relaxed access controls.
Access Control	Enforces granular access control. Users and devices are granted only the minimum privileges required to perform their specific tasks. Access is constantly monitored and can be revoked dynamically based on changing circumstances.	Relies on role-based access control (RBAC). Users are assigned roles with predefined permissions, granting access to specific resources within the trusted zone.
Network Segmentation	Leverages micro-segmentation to further isolate resources and limit lateral movement within the network. Even authorized users may only access specific segments relevant to their tasks.	Typically less granular and focuses on isolating specific network sections (e.g., DMZ) rather than individual resources.
Focus	Prioritizes continuous verification and least privilege access. It assumes breaches can occur and focuses on minimizing damage by limiting access to compromised resources.	Emphasizes preventing unauthorized access at the network perimeter. It aims to create a secure internal zone where traditional access controls can be relaxed.
Scalability	Scales well for dynamic and cloud-based environments. The focus on micro-permissions and least privilege simplifies access management for distributed resources.	Complex as the network grows or adopts cloud services. Managing access control lists for a large user base at the perimeter can be cumbersome.
Implementation	Complex to implement and requires a cultural shift within organizations accustomed to traditional perimeter security.	More established model with readily available security tools and technologies. Implementation is generally easier but may require upgrades to existing infrastructure.