Project:
Securing the Perimeter

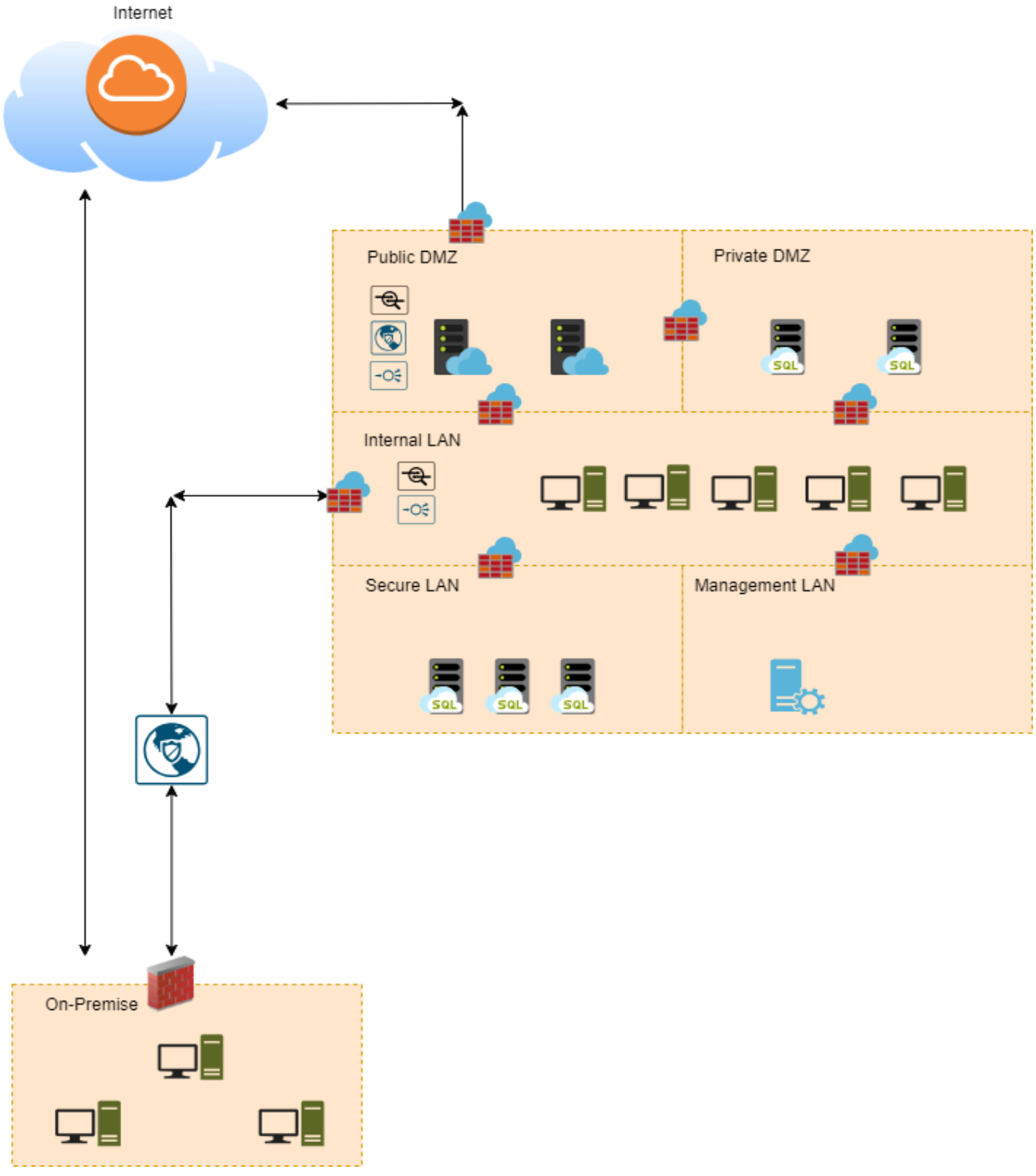
Yaser Issa Ahmed

04/21/2024

Section 1

Designing a Secure Network Architecture

1.1 Designing the Network

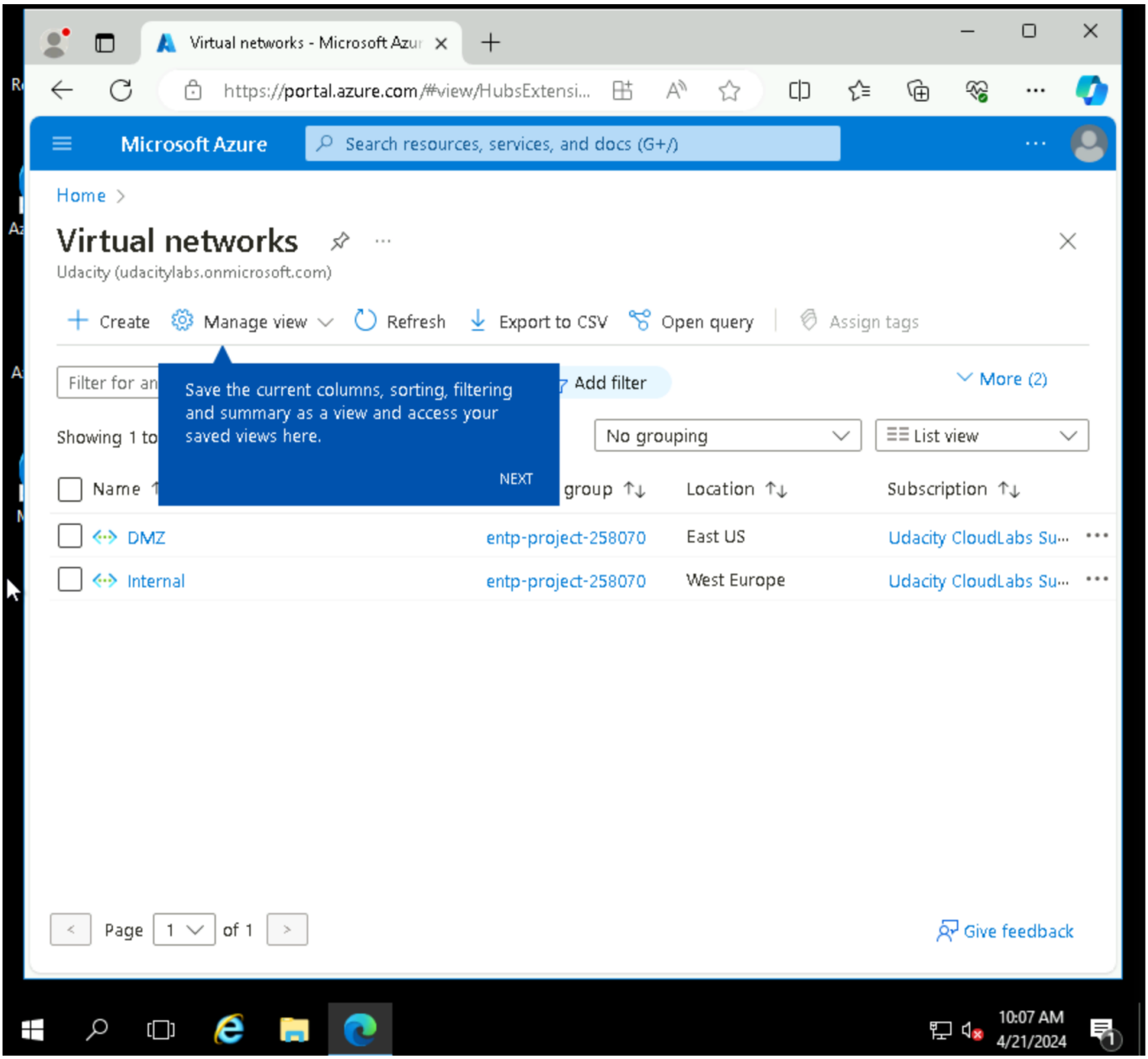


Section 2

Building a Secure Network Architecture in Azure

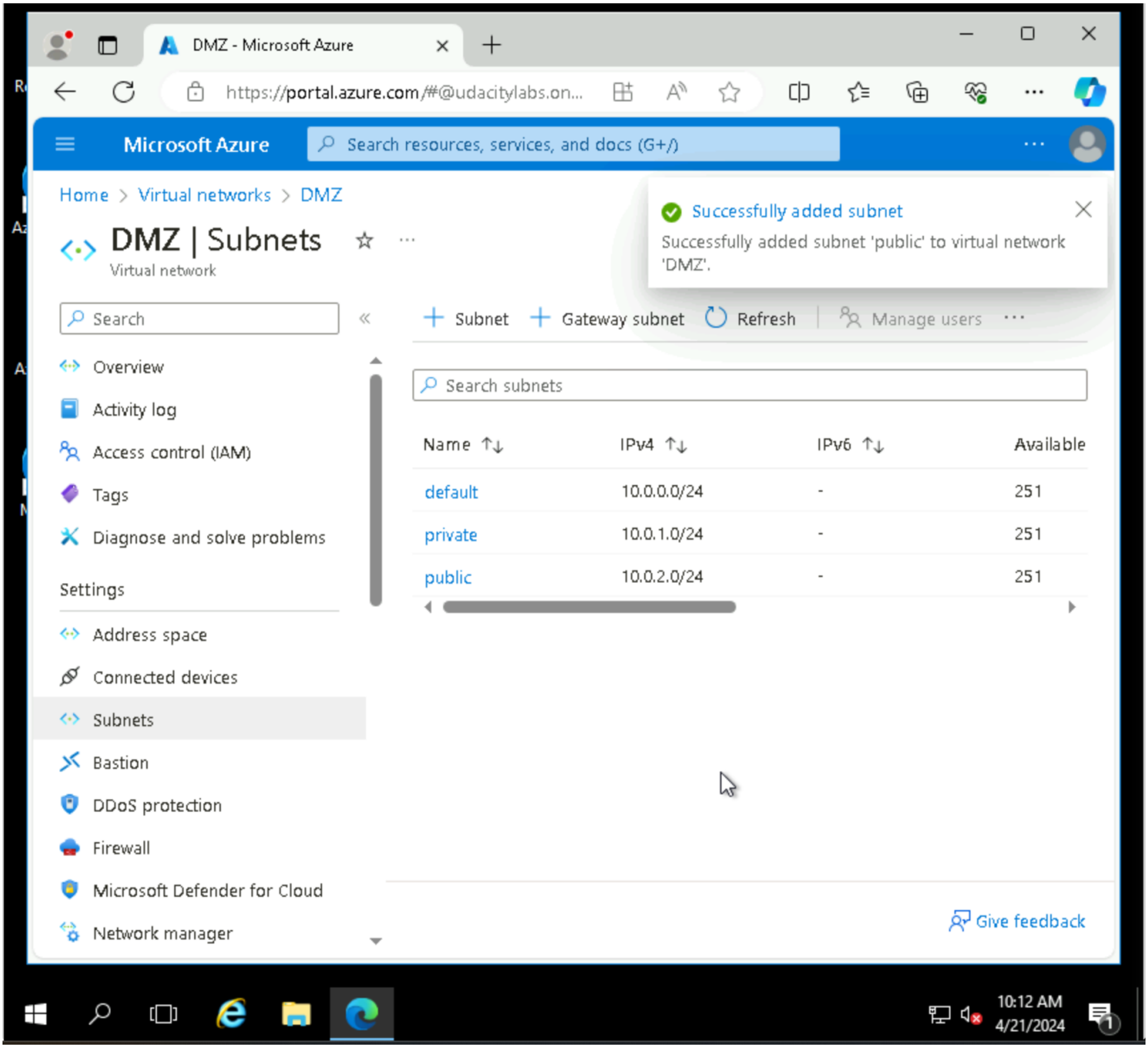
2.1.1 Screenshot

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



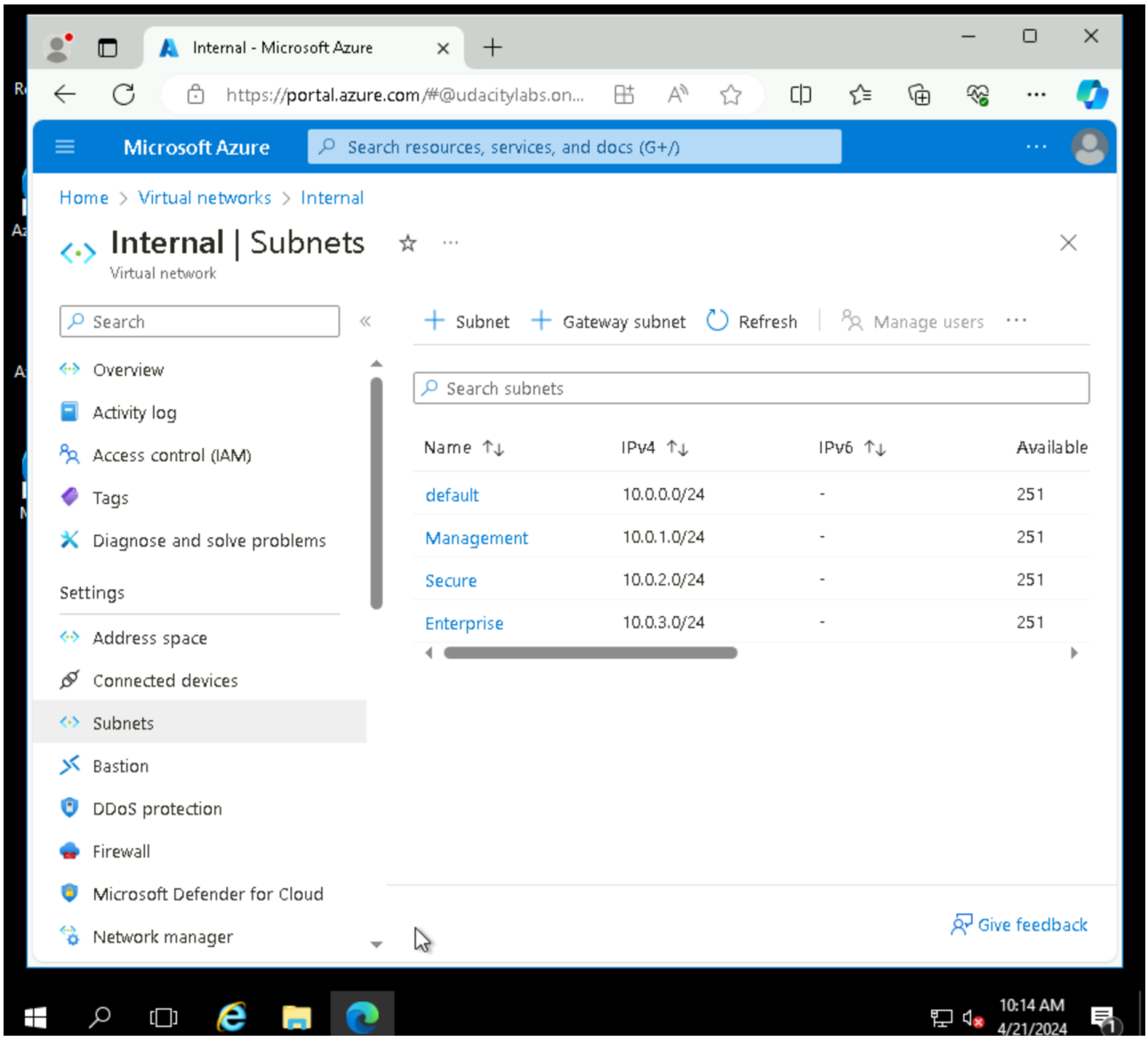
2.1.2 Screenshot

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



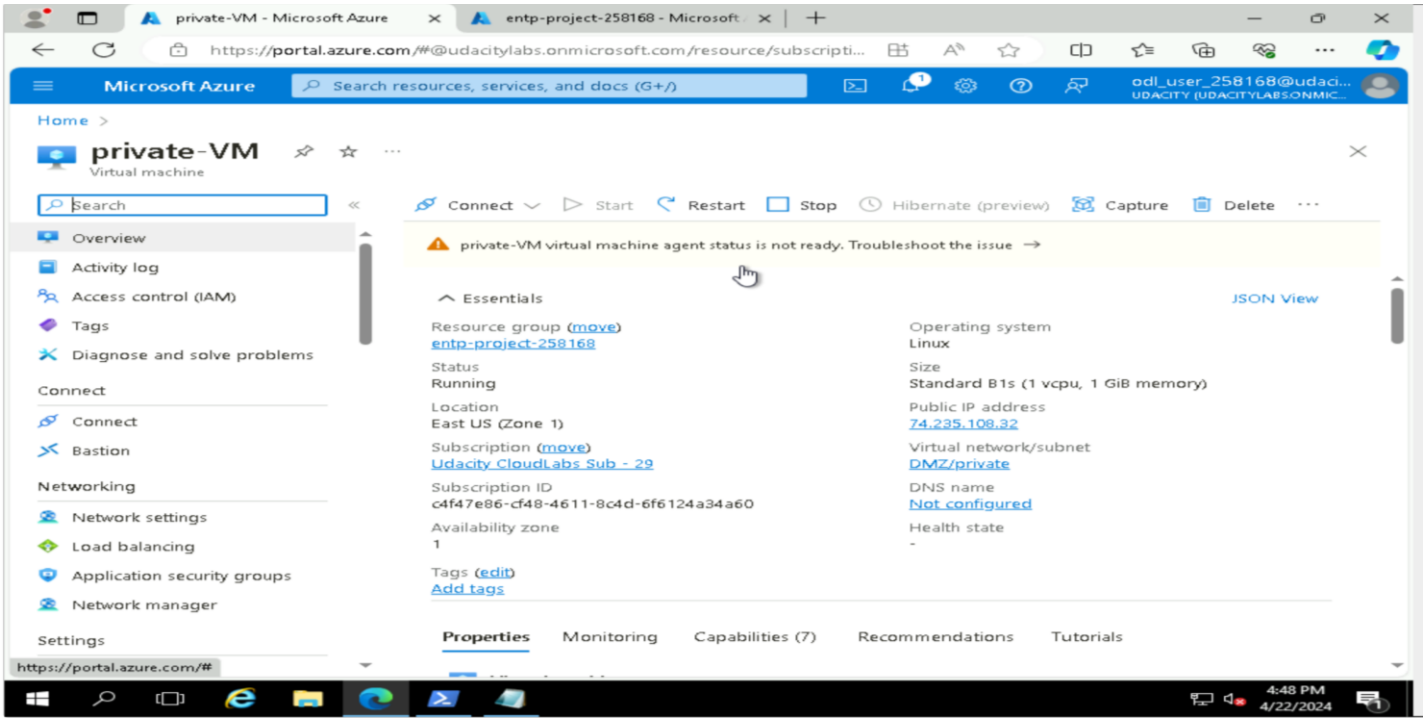
2.1.3 Screenshot

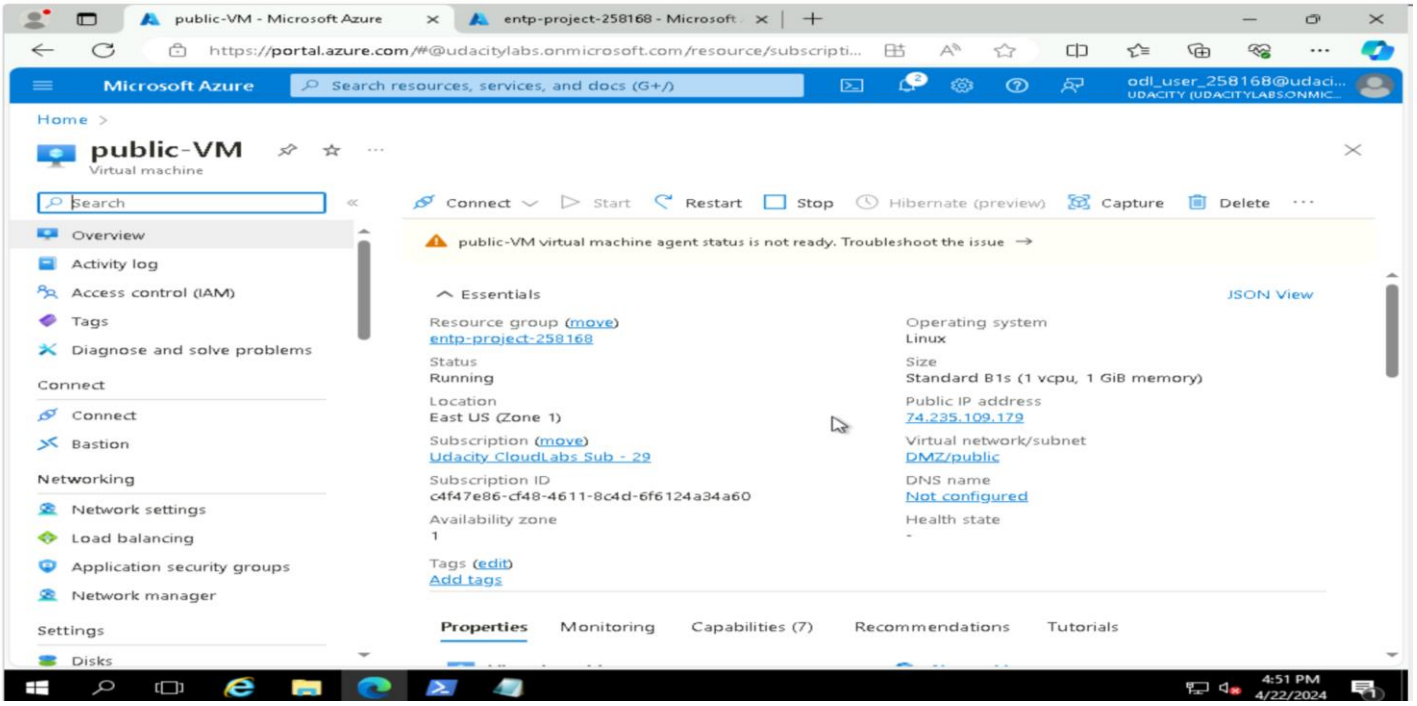
Create three subnets in your internal network and label them Management, Secure, and Enterprise.



2.2.1 Screenshot

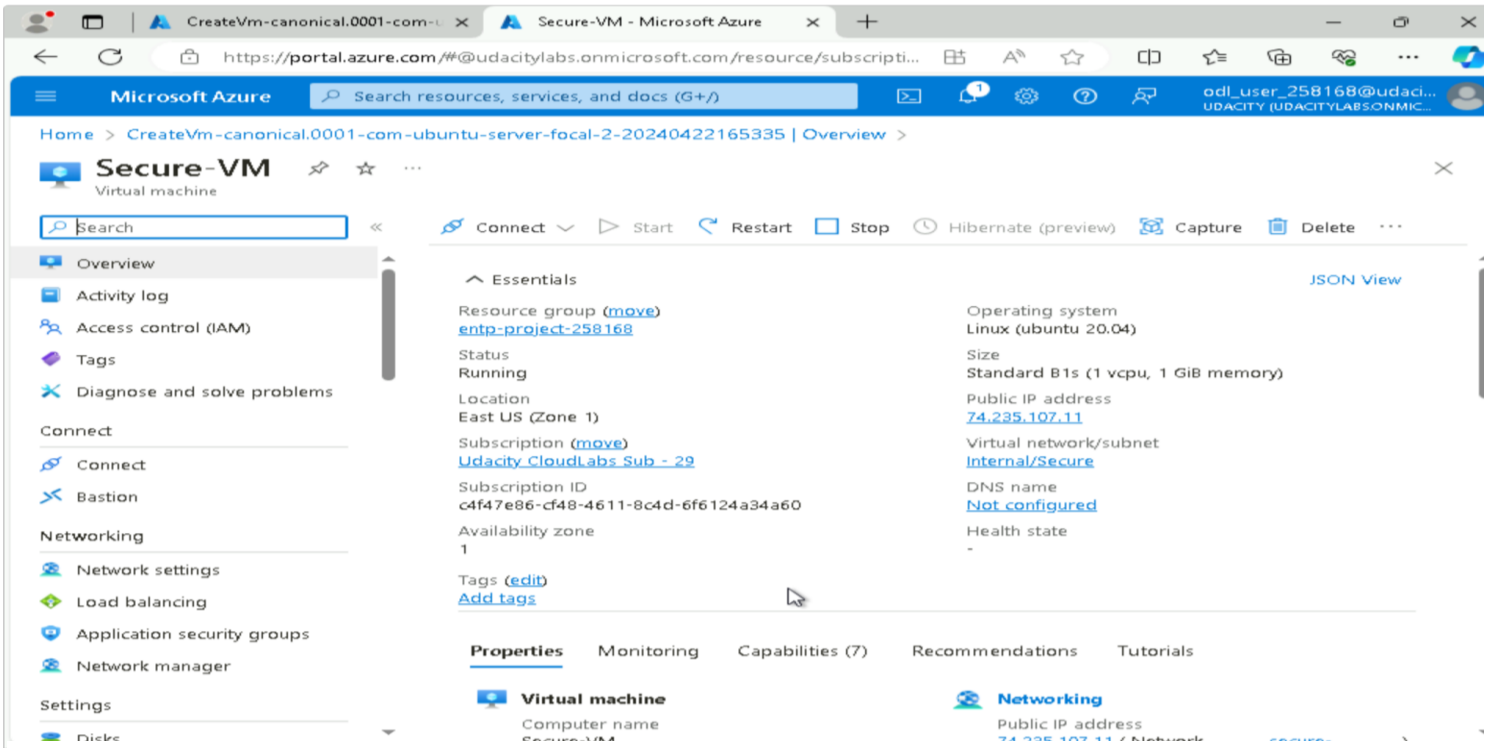
Create one VM in each of your public and private DMZ subnets. Please only use Standard_B1s for your VM size and select the Linux Ubuntu 18.04 image, otherwise you will encounter an error.

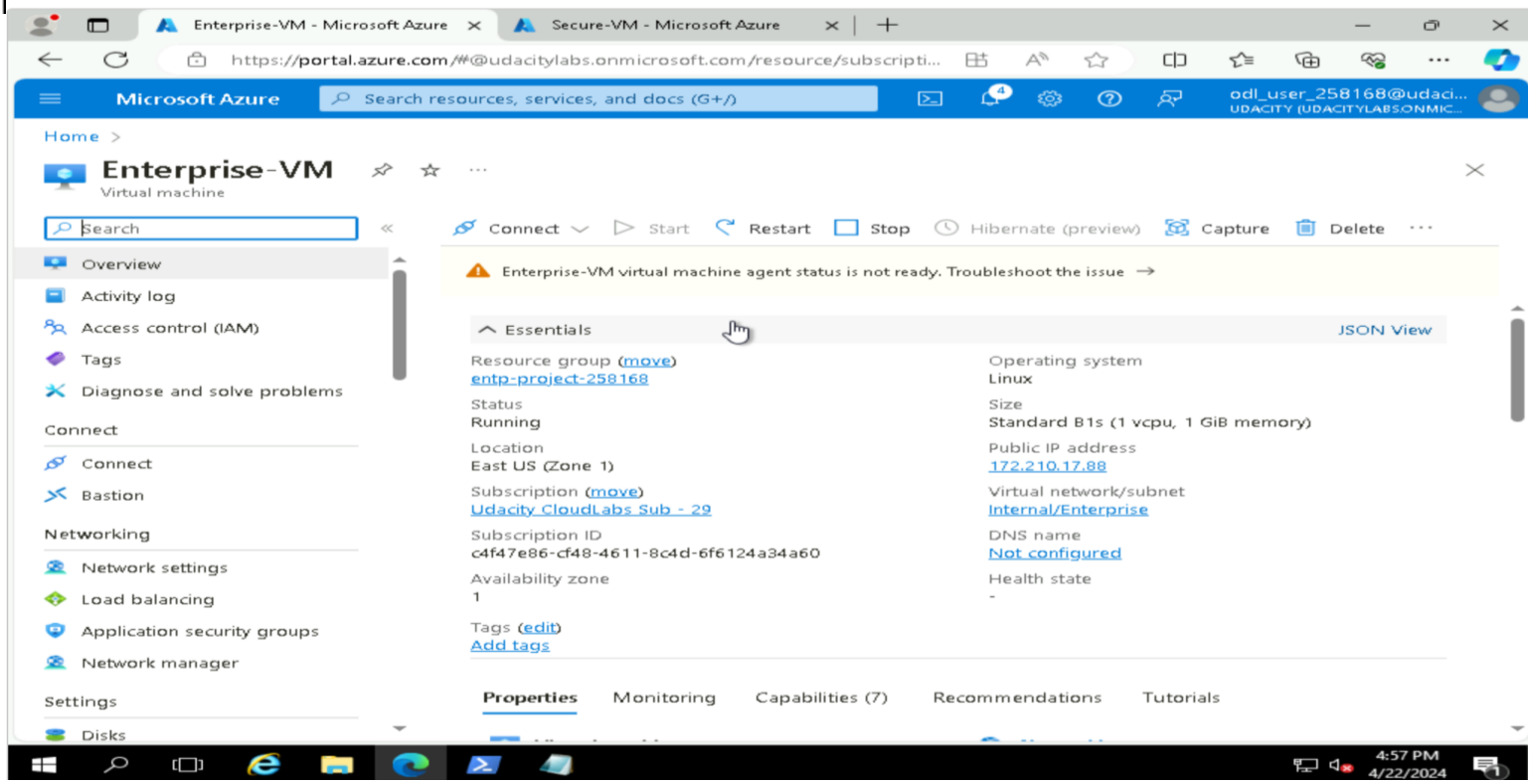




2.2.2 Screenshot

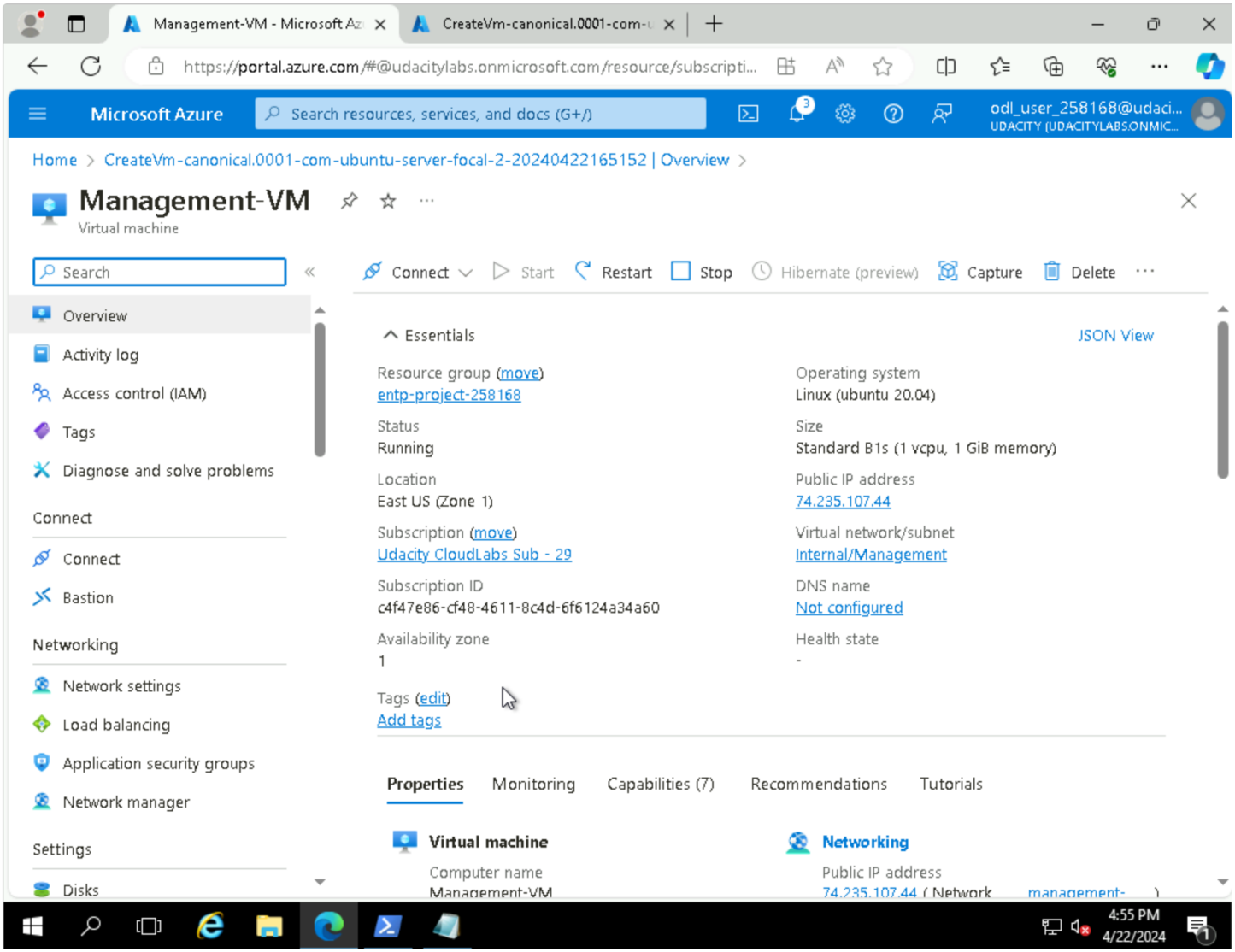
Create one VM in each of your Management, Secure, and Enterprise internal subnets. Please only use Standard_B1s for your VM size and select the Linux Ubuntu 18.04 image, otherwise you will encounter an error.





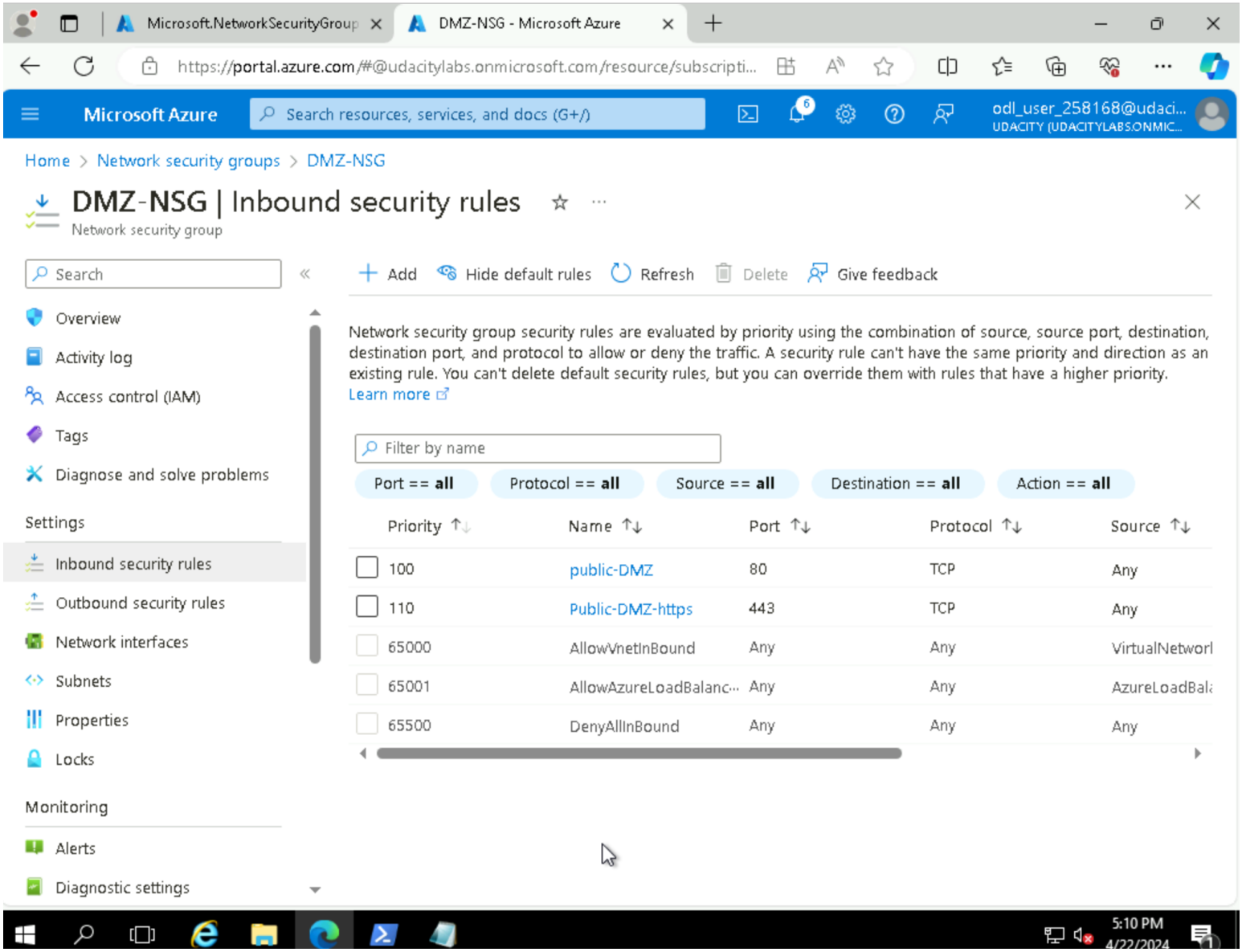
2.2.2 Screenshot

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.



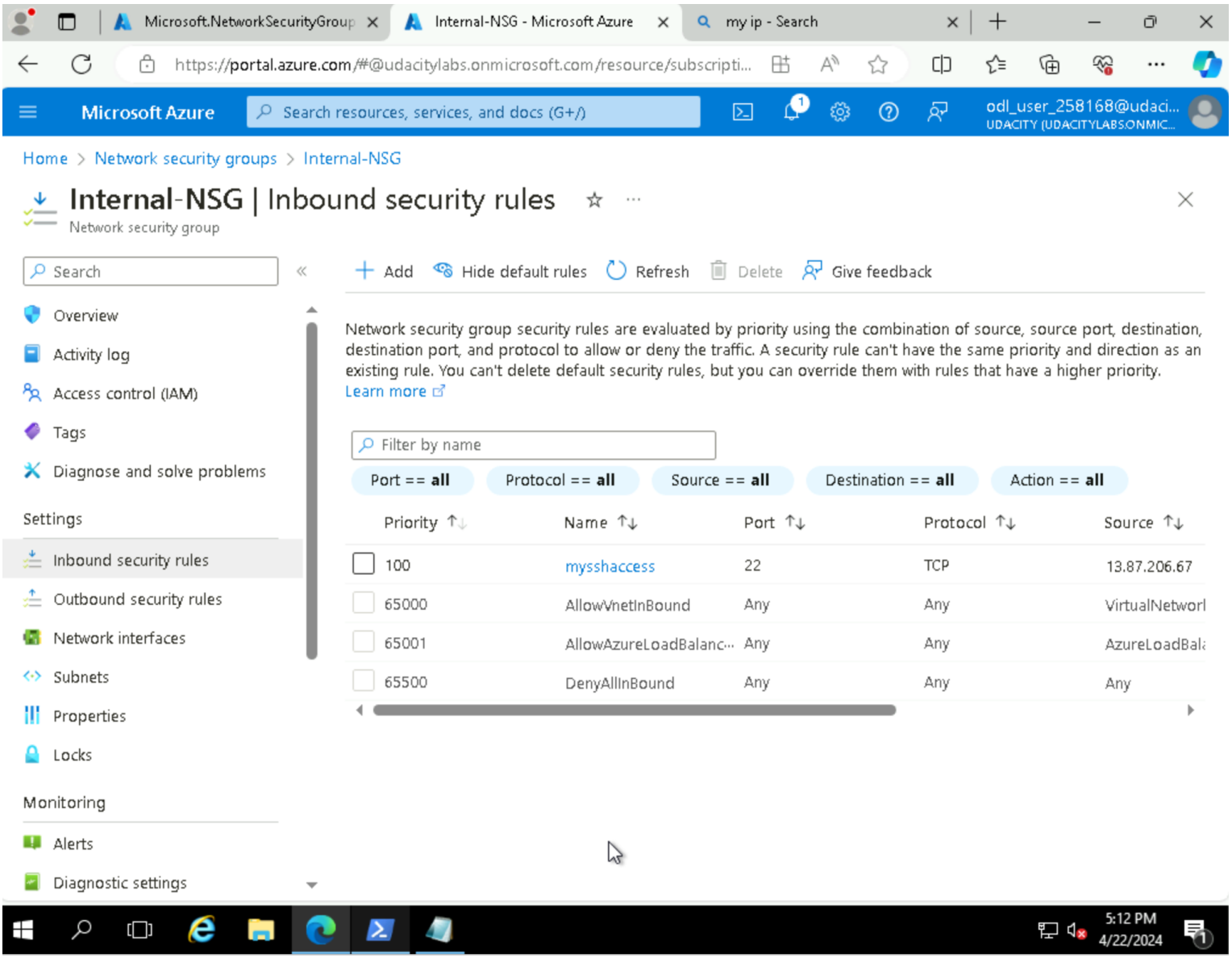
2.3.1 Screenshot

Traffic rules in your DMZ.



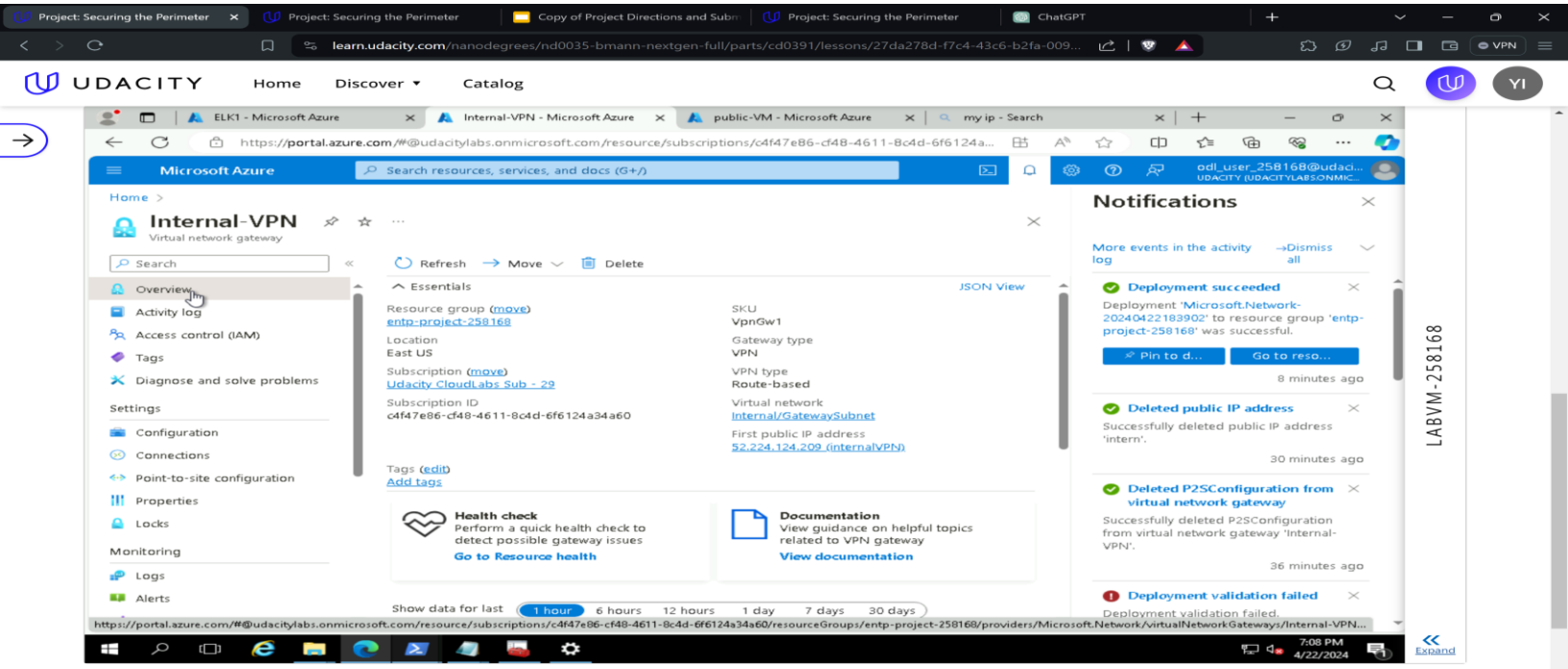
2.3.2 Screenshot

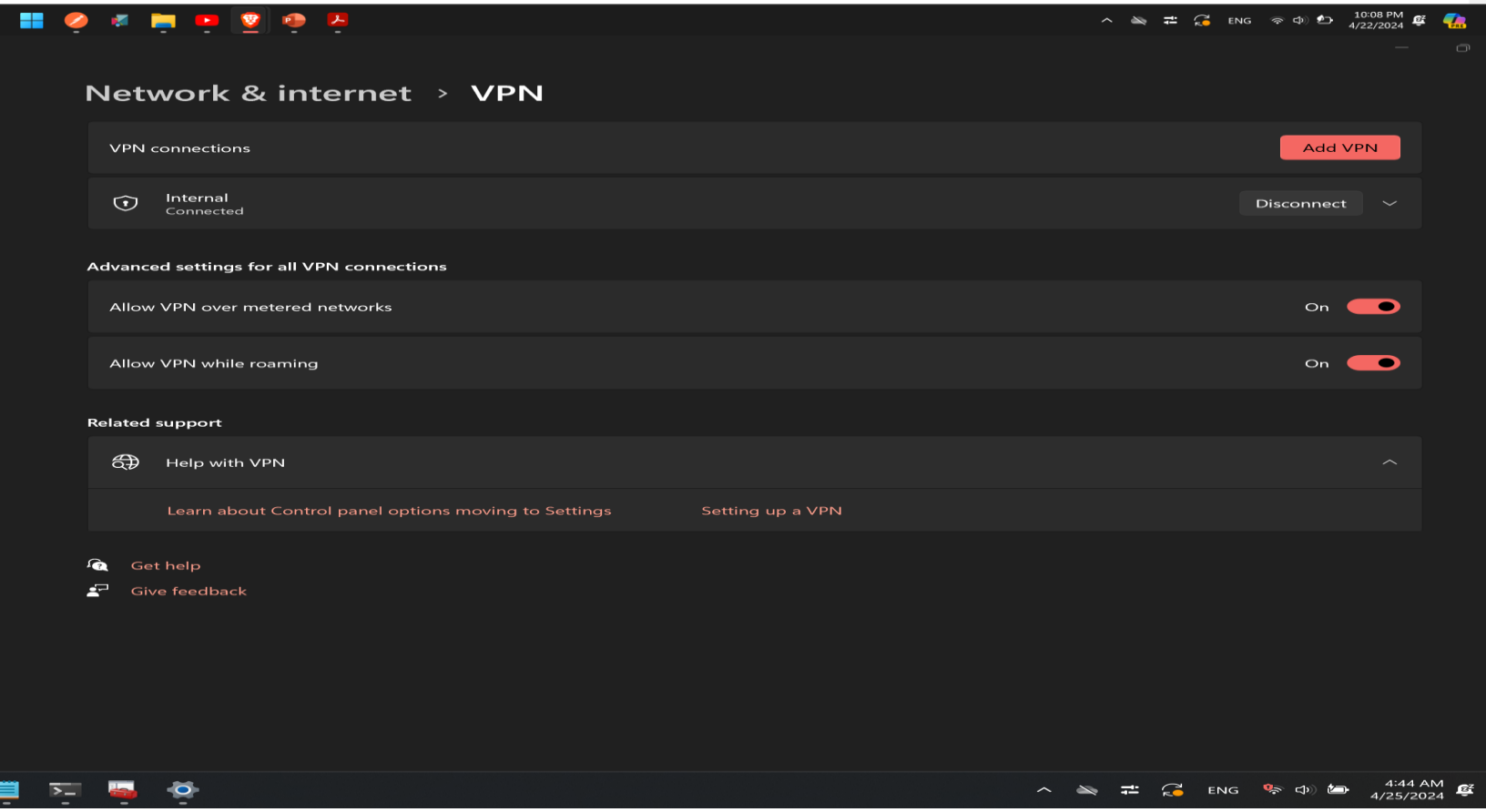
Traffic rules in your Internal network.



2.4.1 Screenshot

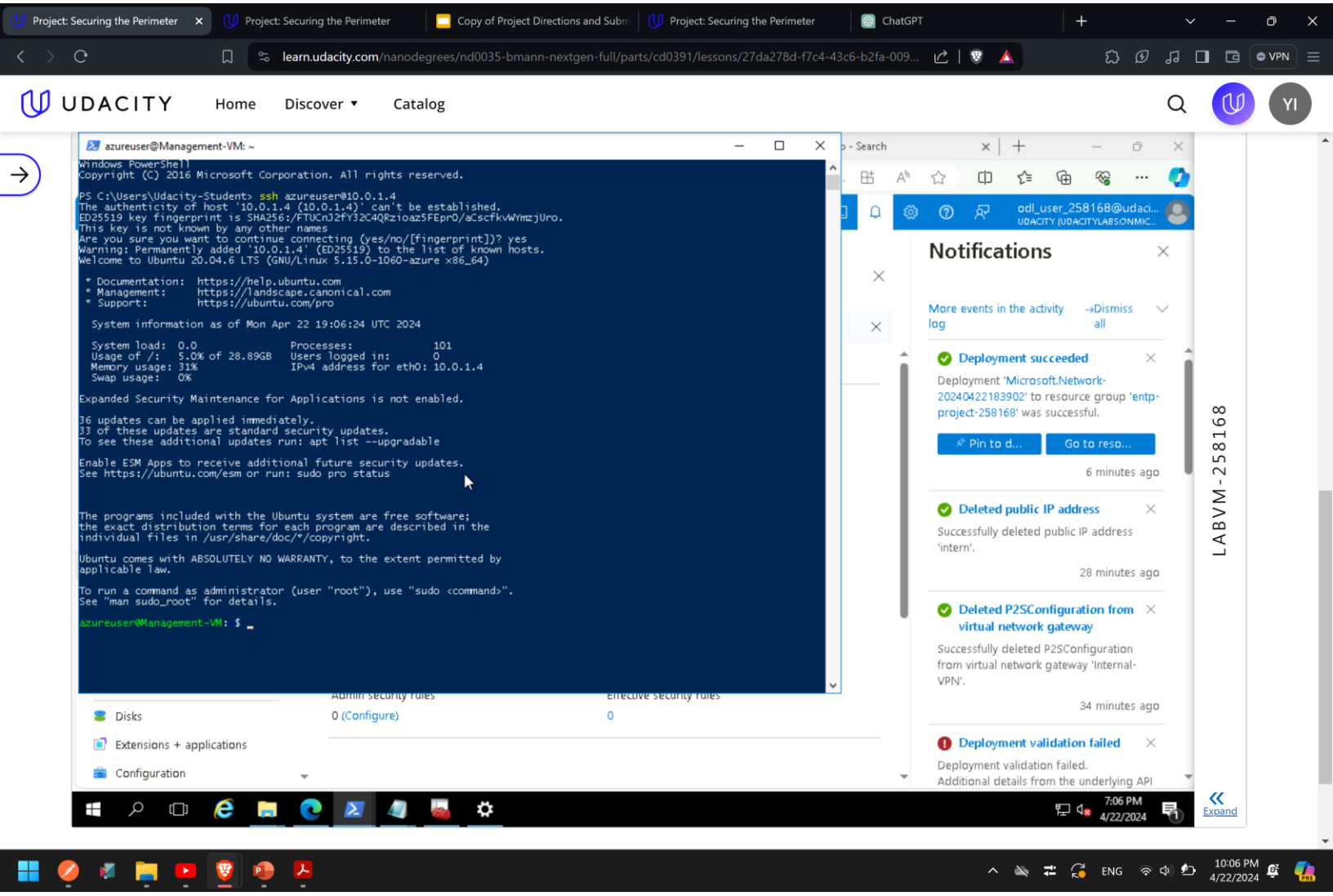
Create a VPN to connect to your internal network.





2.4.2 Screenshot

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

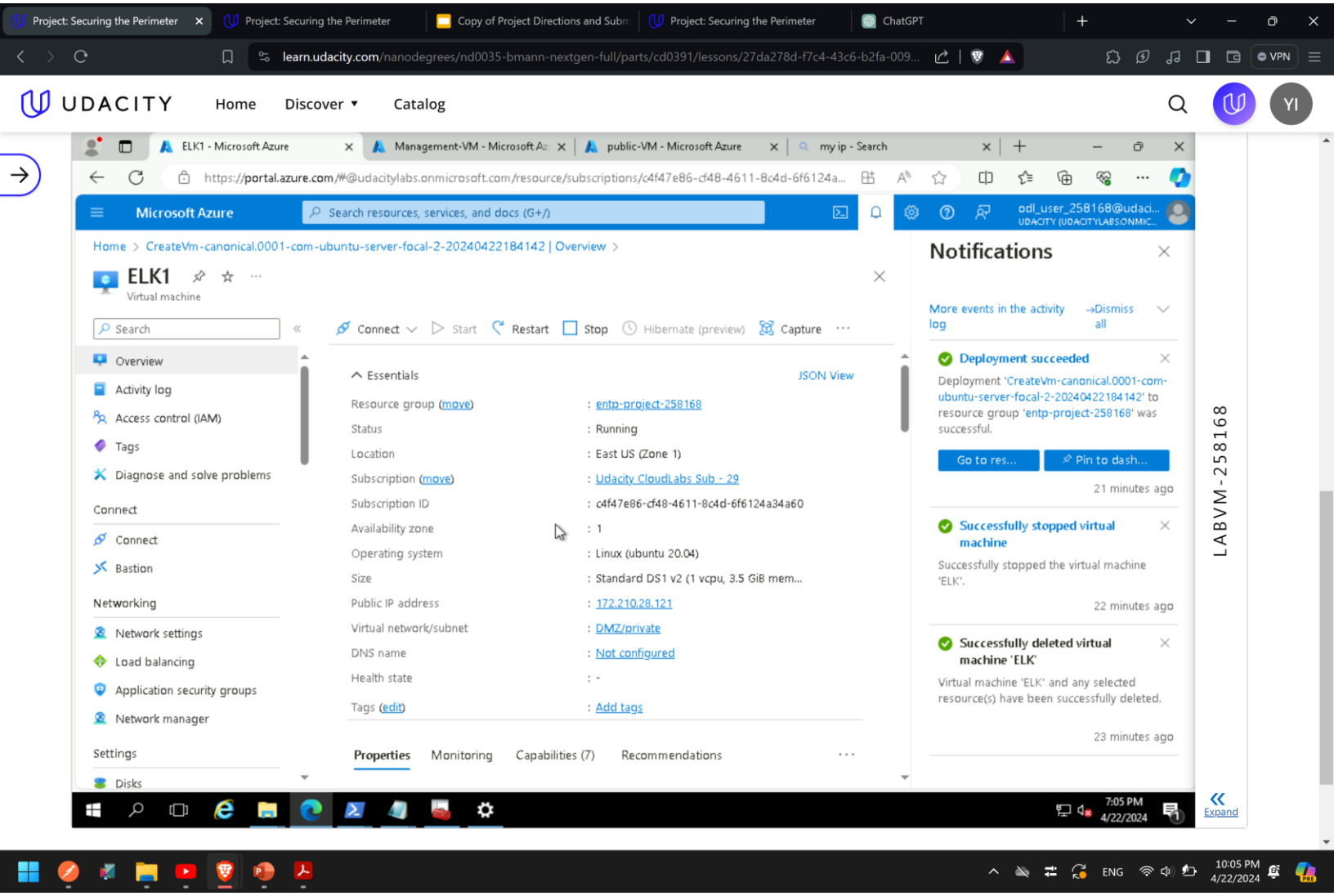


Section 3

Continuous Monitoring with a SIEM

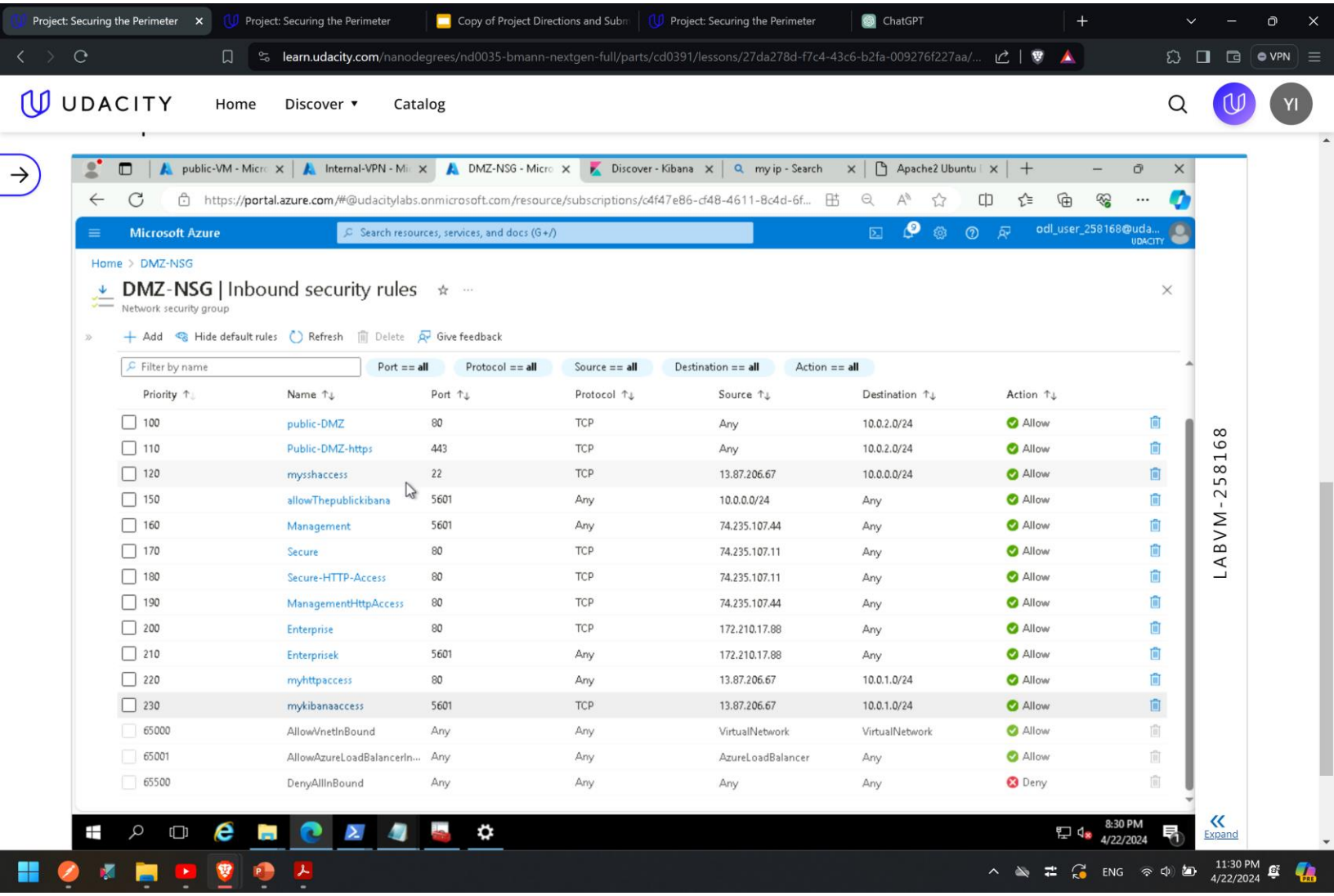
3.1.1 Screenshot

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.



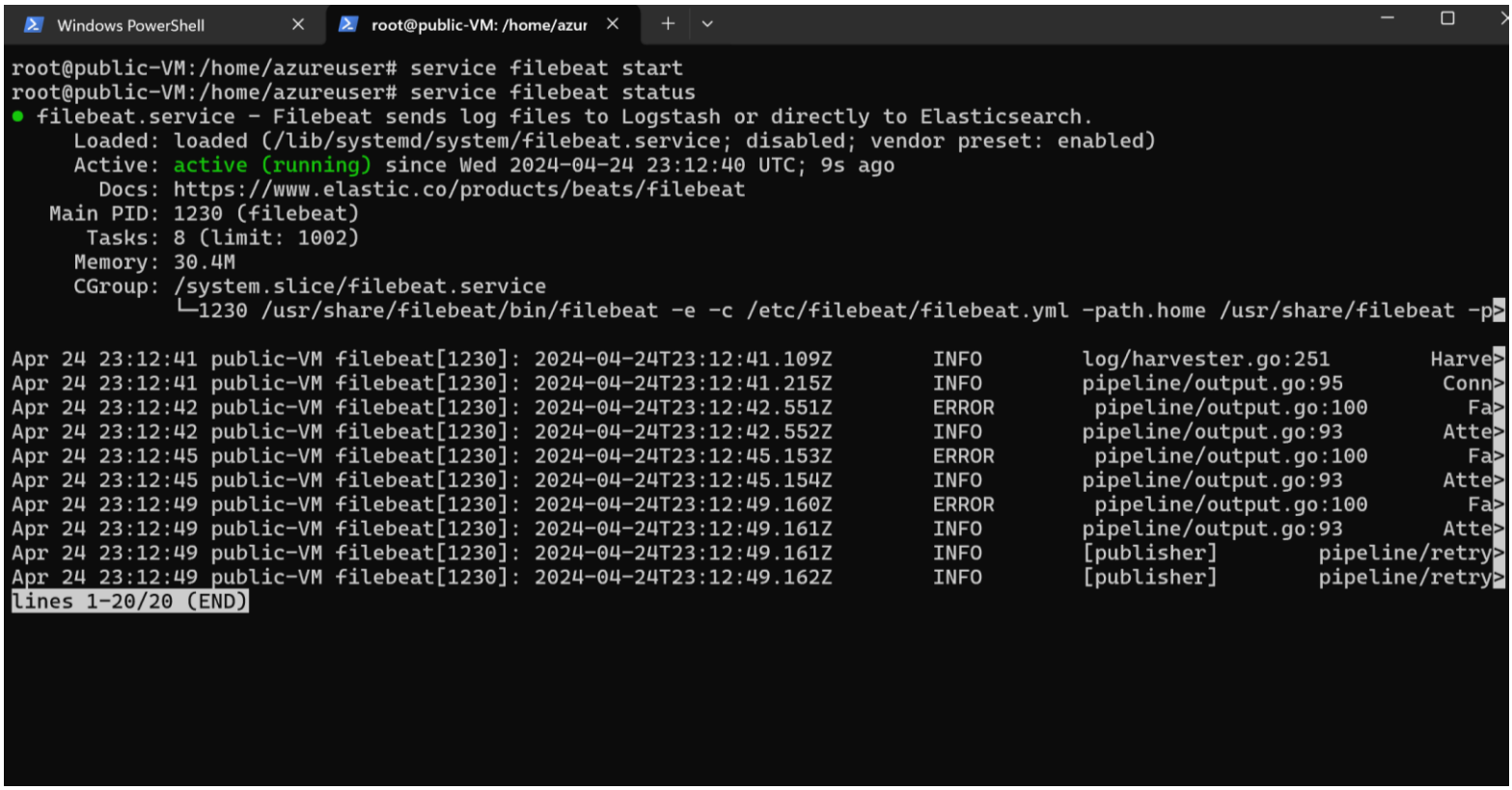
3.1.2 Screenshot

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.



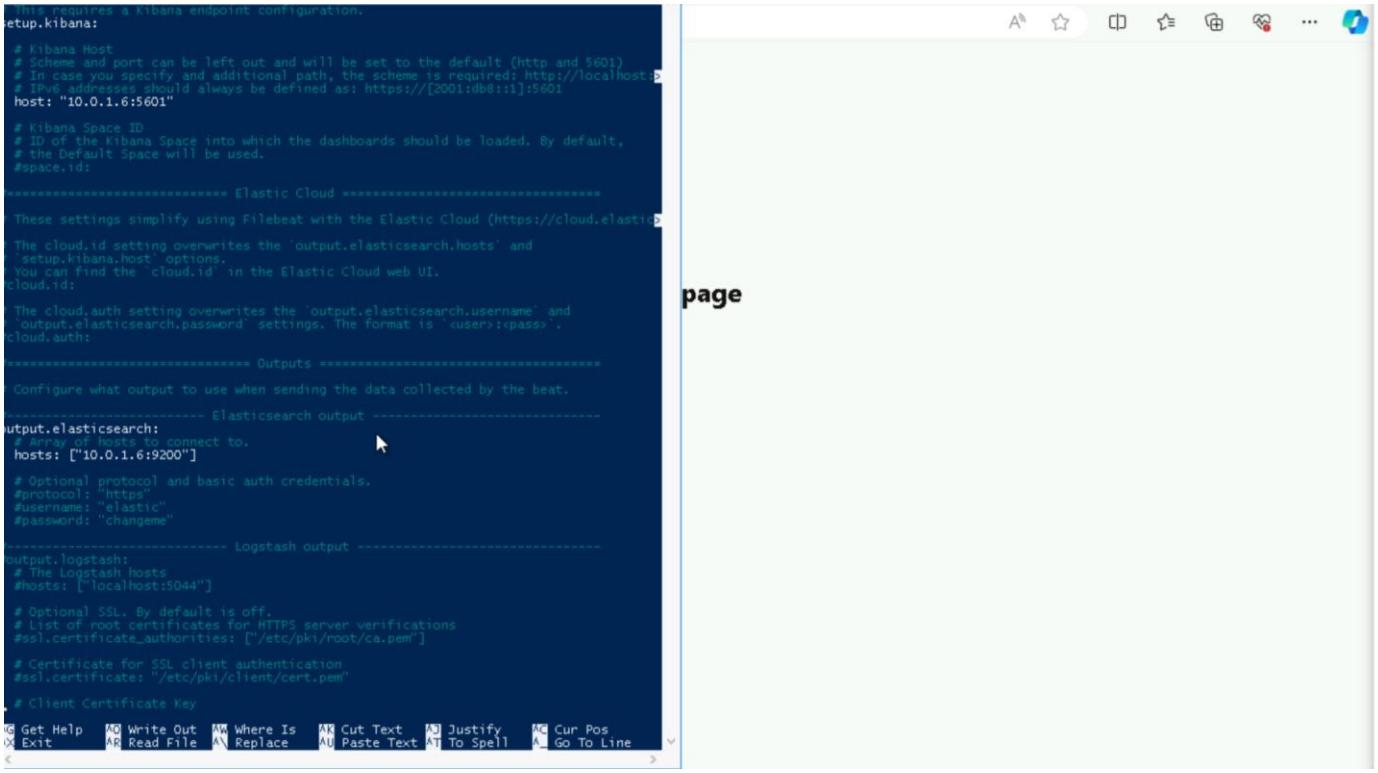
3.2.1 Screenshot

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



3.2.2 Screenshot

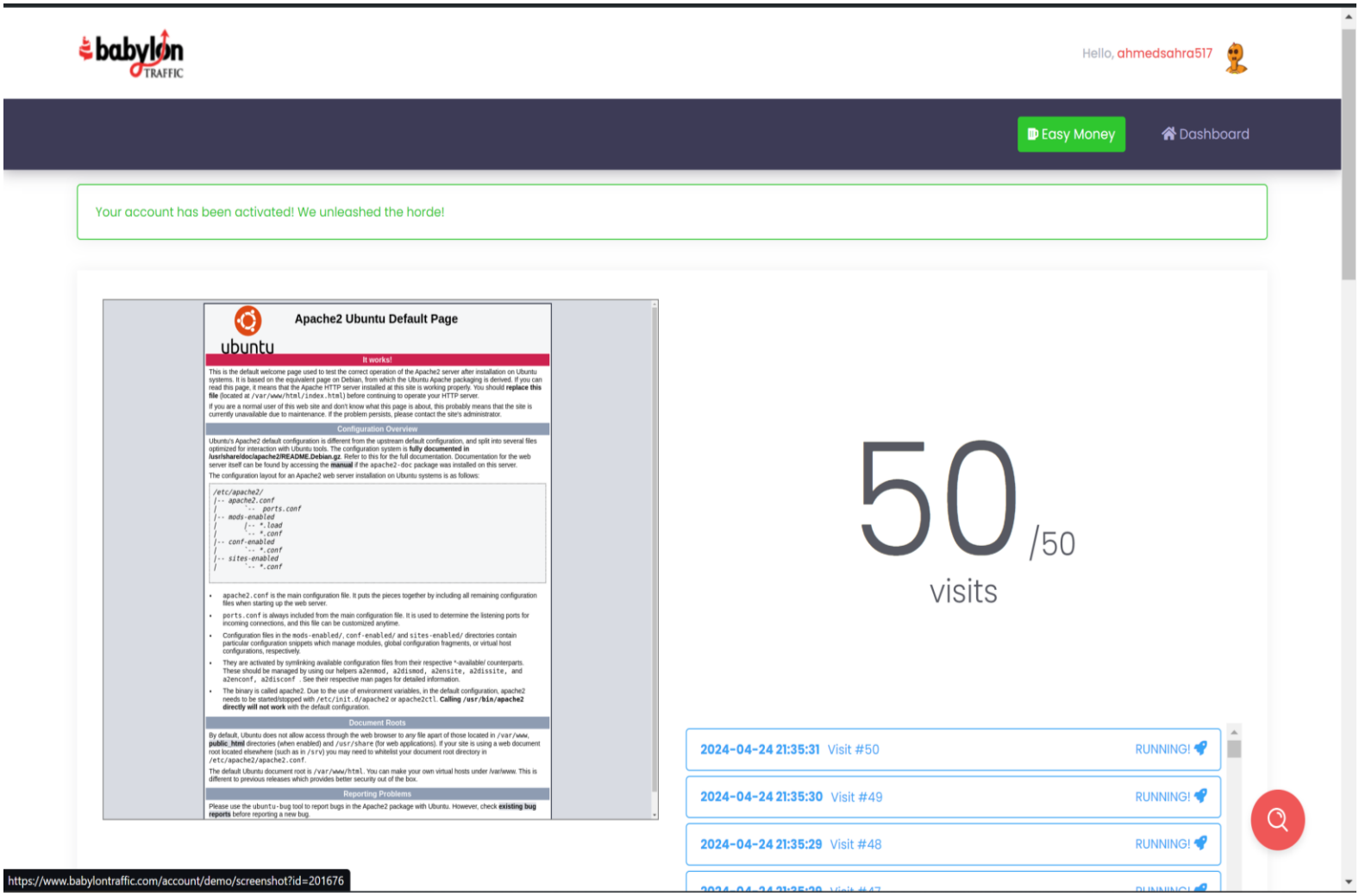
Configure Filebeat to route web server logs to Elasticsearch.



LABVM-258168

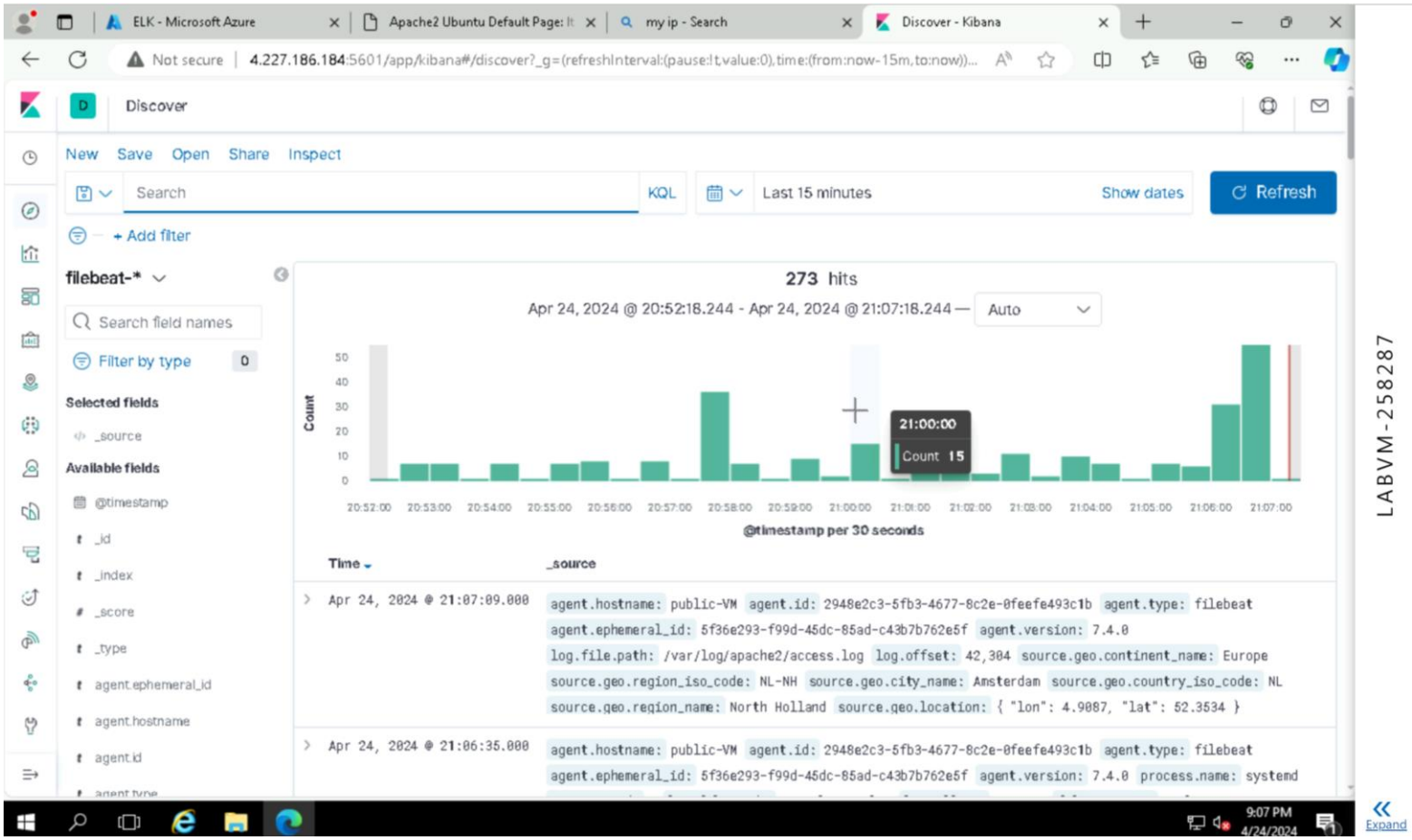
3.2.3 Screenshot

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



3.2.4 Screenshot

Web server logs appear in Kibana.



LABVM-258287

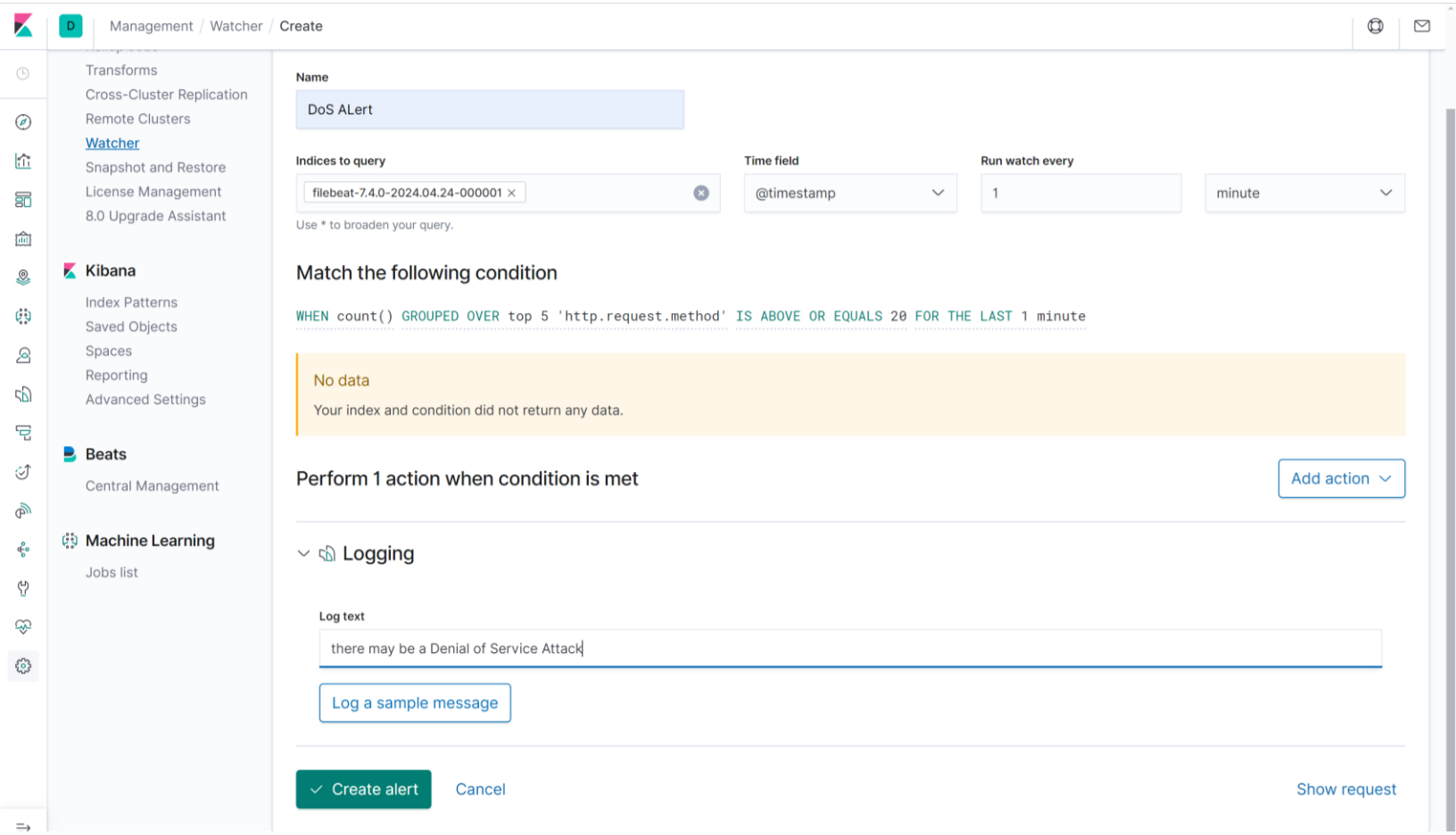
3.3 Build Alerts

In this next section, you will create alerts on the simulated web traffic you see. Build alerts to alert you of possible DoS, brute force, and probing attacks.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

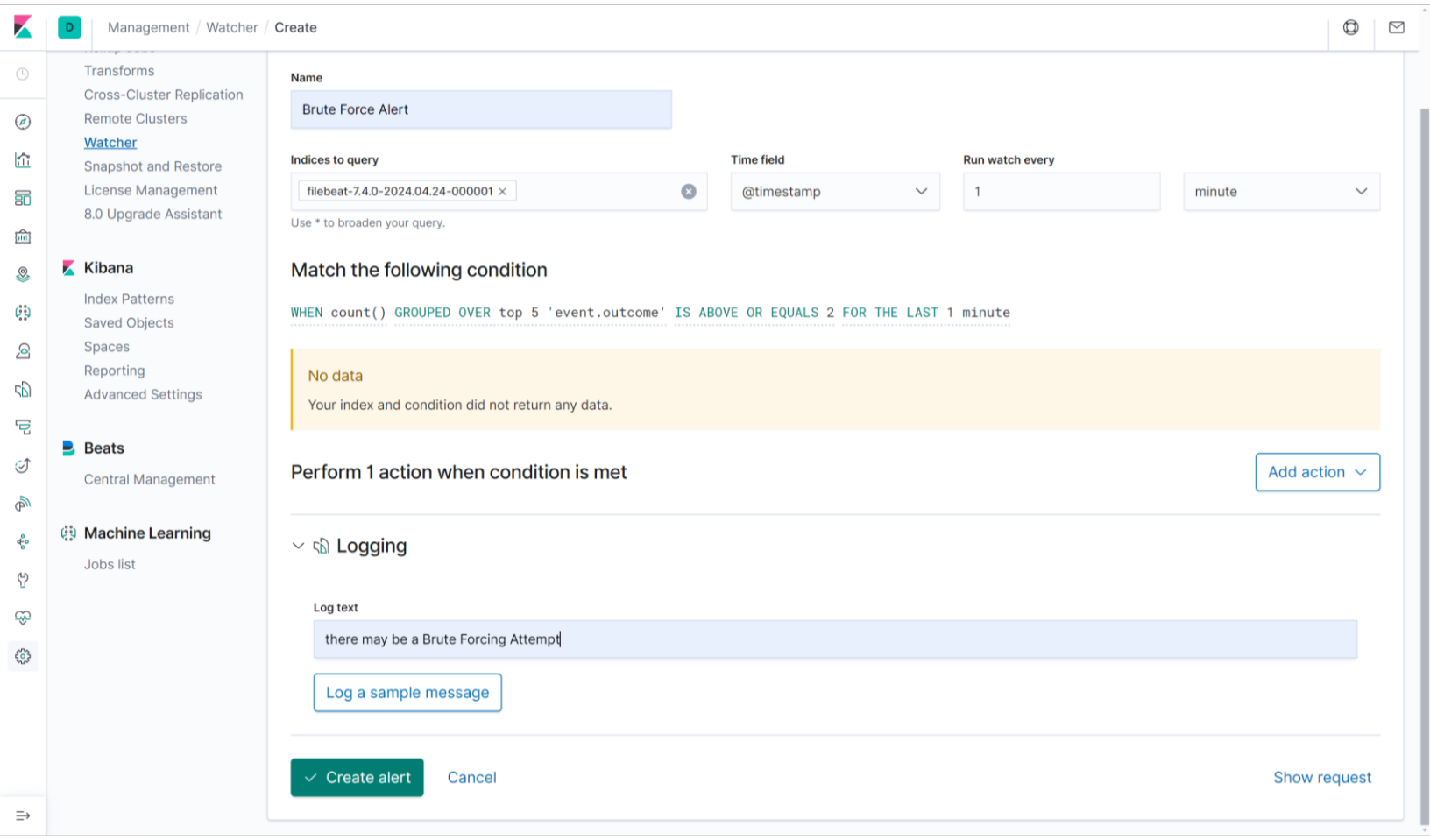
3.3.1 Screenshot

Create an alert for DoS attack.



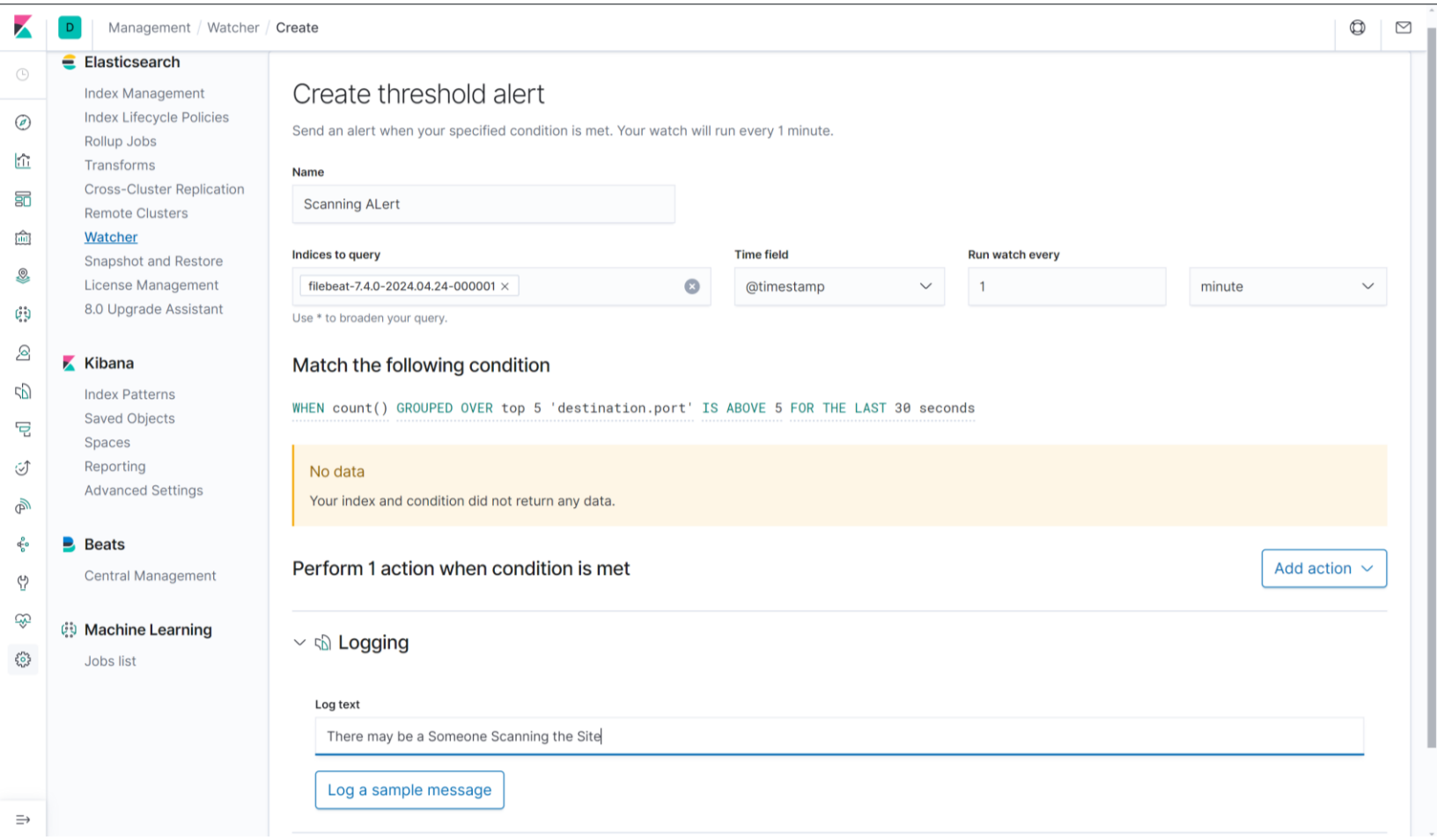
3.3.2 Screenshot

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.



3.4 Incident Response Playbook

1) DoS Attack:

Rate Limiting: Implement rate limiting on the server to restrict the number of requests it can handle within a given timeframe. This helps prevent the server from being overwhelmed by too many requests.
Block List: Identify the IPs sourcing the attack by analyzing logs and network traffic. Once identified, block these IPs at the network level to stop the attack traffic from reaching the server.
Traffic Analysis: Analyze incoming traffic to identify patterns specific to the DoS attack. Look for common characteristics such as high request rates from particular IPs or unusual traffic spikes.
Resource Scaling: Temporarily scale up server resources such as CPU, memory, and bandwidth to handle the increased load caused by the attack. This can help mitigate the impact on service availability until the attack is resolved.

3.4 Incident Response Playbook

Remediation:

Review and update server configurations to optimize performance and mitigate future DoS attacks.
Implement DDoS protection services or appliances to detect and mitigate similar attacks in real-time.

2) Brute Force Attack:

Account Lockout Policies: Implement account lockout policies to automatically lock out user accounts after a certain number of failed login attempts. This helps prevent attackers from guessing passwords through brute force.
Change Passwords: Prompt affected users to change their passwords immediately to prevent unauthorized access to their accounts. Provide guidance on creating strong, unique passwords.

3.4 Incident Response Playbook

Monitor for Suspicious Activity: Continuously monitor system logs and authentication records for any unusual login attempts or access patterns. Investigate any suspicious activity promptly.

Remediation:

Enhance authentication mechanisms with multi-factor authentication (MFA) to add an extra layer of security. Educate users on password hygiene and security best practices to minimize the risk of successful brute force attacks.

3) Scanning and Reconnaissance:

Alter Firewall Rules: Analyze incoming traffic patterns and adjust firewall rules to block or restrict traffic from suspicious sources. This helps prevent attackers from conducting further reconnaissance or exploiting vulnerabilities.

3.4 Incident Response Playbook

Honeypots: Deploy honeypots strategically within the network to lure and trap attackers. Analyze the behavior of attackers targeting the honeypots to gather intelligence on their tactics and techniques.

Network Segmentation: Ensure critical assets are isolated within segmented network zones. This limits the potential impact of a successful attack and prevents lateral movement within the network.

Remediation:

Regularly review and update firewall rules to adapt to evolving threats and attack techniques.
Conduct periodic security assessments and penetration tests to identify and address vulnerabilities in the network infrastructure.

Section 4

Designing a Zero Trust Model

Section 4: Zero Trust Model

XYZ is elated with the work you've done so far! But they've been hearing about this new buzzword "Zero Trust" and are curious as to what it is and what the architecture would look like in a Zero Trust model. So your next task below is to design a Zero Trust model, then explain the differences between your network architecture and your Zero Trust model.

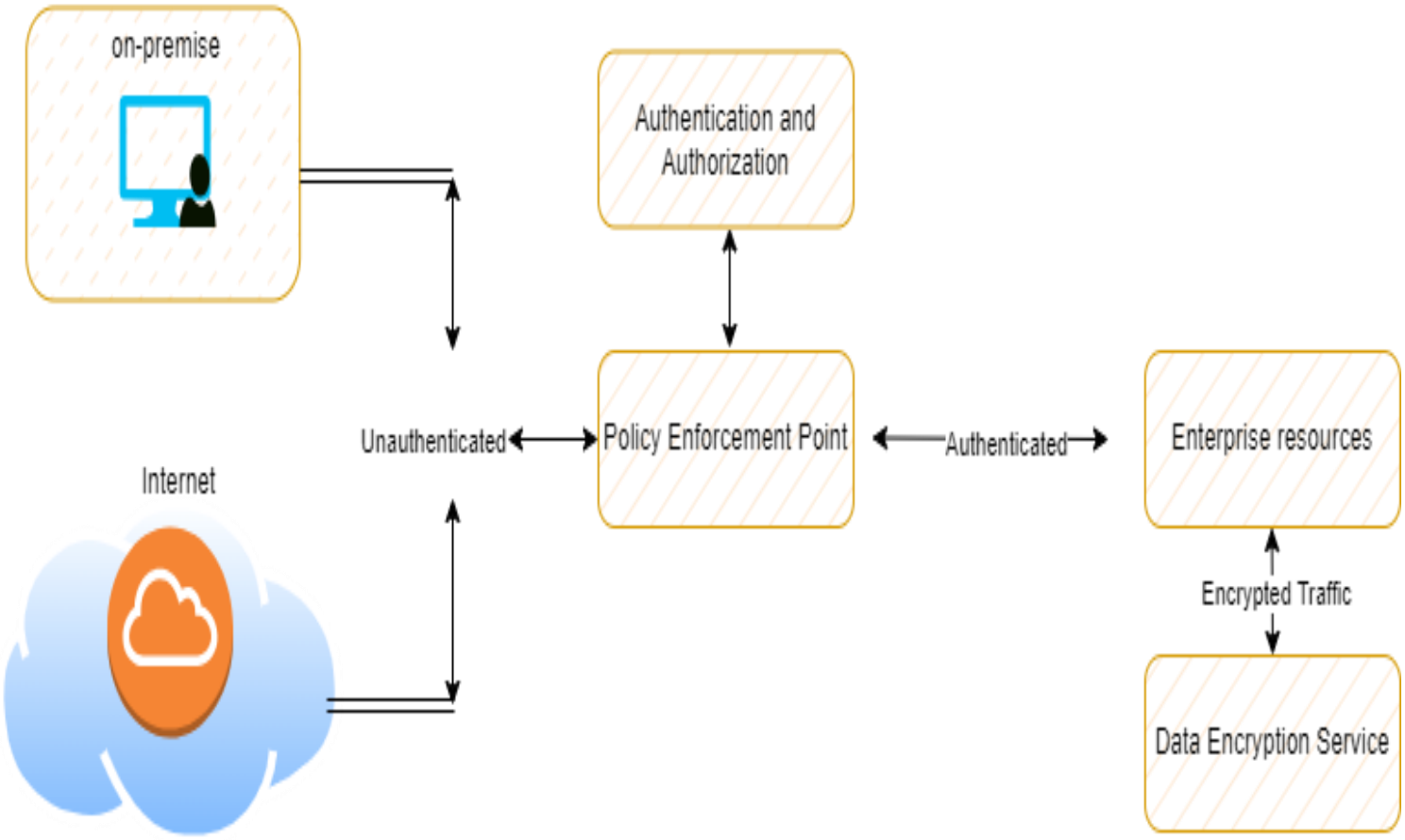
Design a Zero Trust model of your network architecture using https://app.diagrams.net/.

Make sure to incorporate the following into your design:

- Identity
- Devices
- Apps
- Network
- Data
- Infrastructure
- Trusted and Untrusted Devices
- Controls

4.1 Zero Trust Model

Paste your Zero Trust model diagram here:



4.2 Modern Architecture vs. Zero Trust

In my Zero Trust model, authentication serves as the cornerstone of network security, requiring rigorous verification of users, whether they originate from the on-premise network or connect directly from the internet. Before granting access to resources such as the VPN or the Public DMZ, users must undergo an authentication process, to ensure their identities are validated. This approach mitigates the risk of unauthorized access attempts and strengthens the overall security posture of the network.

Furthermore, encryption plays a pivotal role in safeguarding data integrity and confidentiality throughout the entire system. All traffic flowing within the network, whether between segments or from external sources, is encrypted to prevent any eavesdropping. This aligns with the Zero Trust principle of assuming breach and implementing robust data protection measures.

Additionally, the concept of trust is redefined within this model, moving away from implicit trust based on network location to continuous verification of identity and behavior. Trust is never assumed and must be earned through ongoing authentication and authorization processes. This contrasts with traditional network architectures that rely heavily on perimeter-based trust models.

4.2 Modern Architecture vs. Zero Trust

Moreover, the emergence of cloud services has rendered traditional perimeter defenses outdated, necessitating a shift towards a Zero Trust mindset. Modern network architectures must adapt to the dynamic nature of cloud environments by implementing granular access controls and encryption mechanisms that transcend traditional network boundaries.

Finally, the evolution of the threat landscape underscores the importance of adopting a Zero Trust approach. With increasingly sophisticated cyber threats, organizations can no longer rely solely on perimeter defenses but must instead adopt proactive security measures that continuously monitor and respond to threats in real-time.