UDACITY

Securing the Perimeter

EMMANUEL AVAH

17-05-2024

Project Scenario

Overview

XYZ is the premier cryptocurrency exchange. They transact over a billion trades everyday and are considered to be one of the most reliable and secure exchanges in the world. Due to their rapid growth, they've faced challenges in scaling their security posture. The largest challenge they've faced is with their Perimeter Network Security being secure. The networking team was overburdened with the rapid growth and a majority of the network infrastructure was built insecurely.

Due to a lack of visibility and a lack of proper access control setup on the network, it was inevitable that a breach took place! XYZ was hit with a massive attack in which their network was breached and their internal servers were compromised resulting in over 500 Bitcoin being stolen!

Needing to get the bottom of this breach and resolving their current perimeter issues they've contracted you from SecureCorp, a world renowned cybersecurity consulting firm. Your job is to redesign their network architecture securely and set up a SIEM to monitor against future attacks.

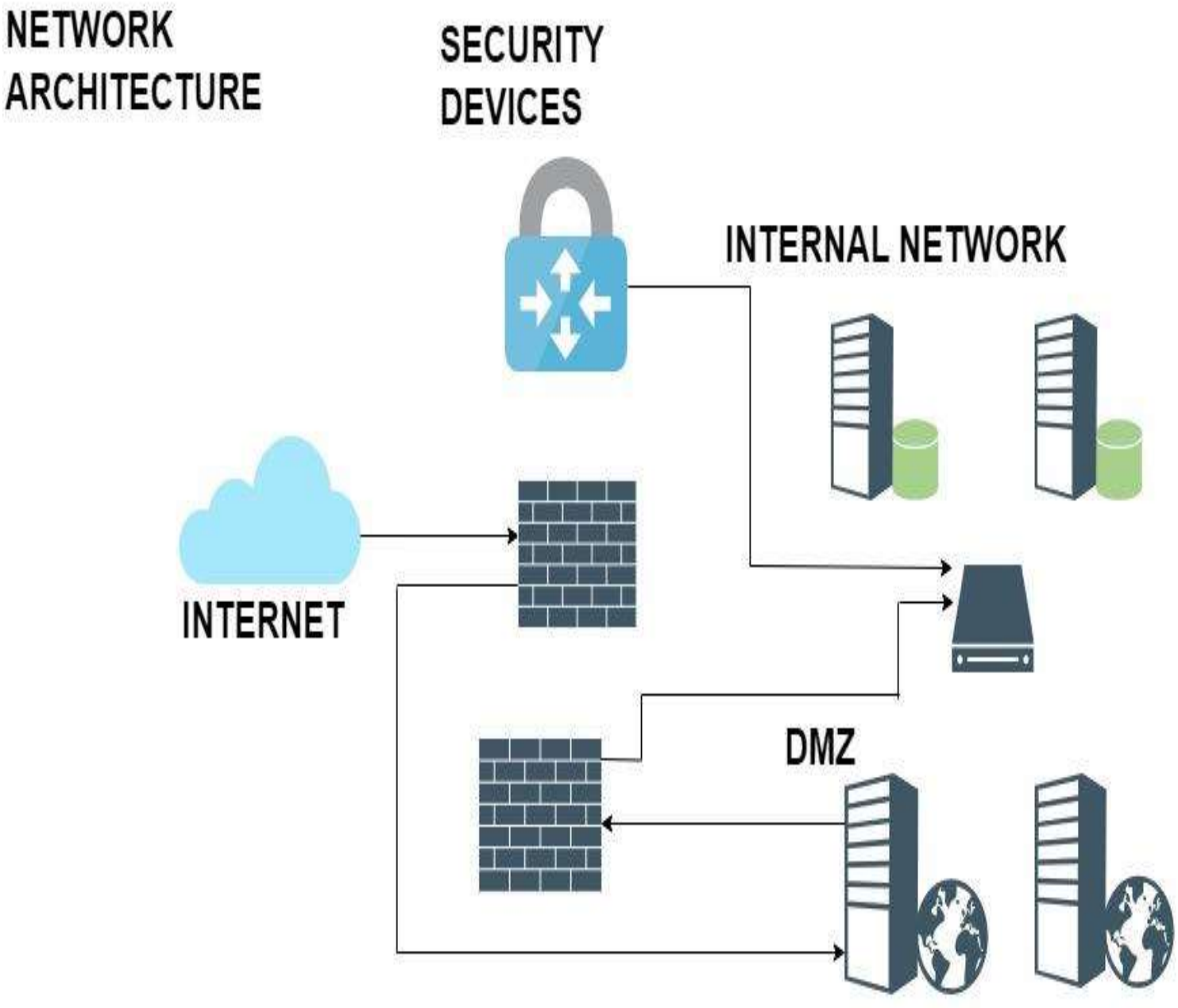
Section One: Designing a Secure Network Architecture

Identify Network Vulnerabilities

1. Lack of Network Segmentation
Problem: The network architecture lacks proper network segmentation, with all five servers residing in a single virtual network and subnet. This design allows direct connectivity between the servers, increasing the attack surface. Risk: Without network segmentation, an attacker who gains access to one server can potentially move laterally and compromise the other servers, including the critical database servers and the file storage server.
2. Excessive Direct Internet Connectivity:
Problem: All servers in the network have direct connections to the internet, increasing the exposure to external threats and bypassing any potential security controls. Risk: Direct internet connectivity for all servers amplifies the risk of network breaches and cyber attacks. Malicious actors can exploit vulnerabilities in the servers or the services running on them to gain unauthorized access, steal sensitive data, or launch further attacks within the network.
3. Inadequate Access Control
Problem: The network description suggests a lack of proper access control mechanisms, particularly in the communication between the web servers and the database servers. Risk: Without robust access control measures, such as role-based access and least-privilege principles, the network is susceptible to unauthorized access and potential data breaches.

Network Redesign

Updated Network Diagram



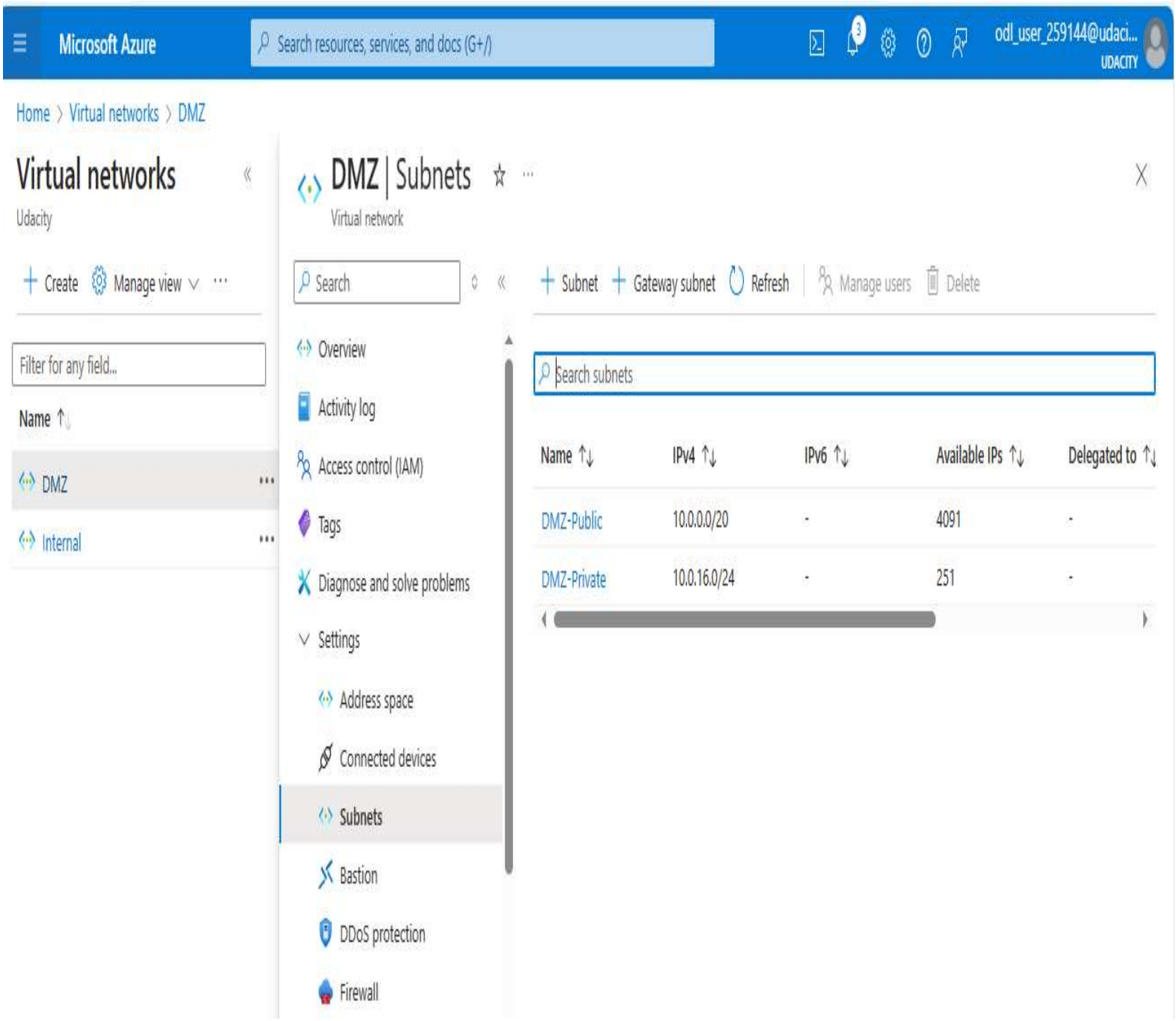
Identify Network Vulnerabilities

Why do we need to add firewalls to our network?
Adding firewalls to the network is a critical security measure for a Cryptocurrency exchange like ours. Firewalls act as the first line of defense, controlling and monitoring the flow of traffic in and out of our network. Here are the key security benefits of implementing firewalls: 1. Enhanced network segmentation 2. Improved threat detection and mitigation 3. Compliance and regulatory requirements 4. Increased network resilience
What is the benefit of having different areas in our network for web servers and database servers?
Separating the web servers and database servers into different network areas, commonly known as a DMZ (Demilitarized Zone) architecture, provides several crucial security benefits for our cryptocurrency exchange: 1. Reduced attack surface 2. Granular access control 3. Improved logging and monitoring 4. Compliance and regulatory benefits
What does a VPN do for our connection to the file storage server?
Establishing a VPN (Virtual Private Network) connection to our file storage server provides several security benefits for our cryptocurrency exchange: 1. Secure data transmission 2. Access control and authentication 3. Compliance and regulatory adherence 4. Centralized management and monitoring

Section Two: Building a Secure Network Architecture in Azure

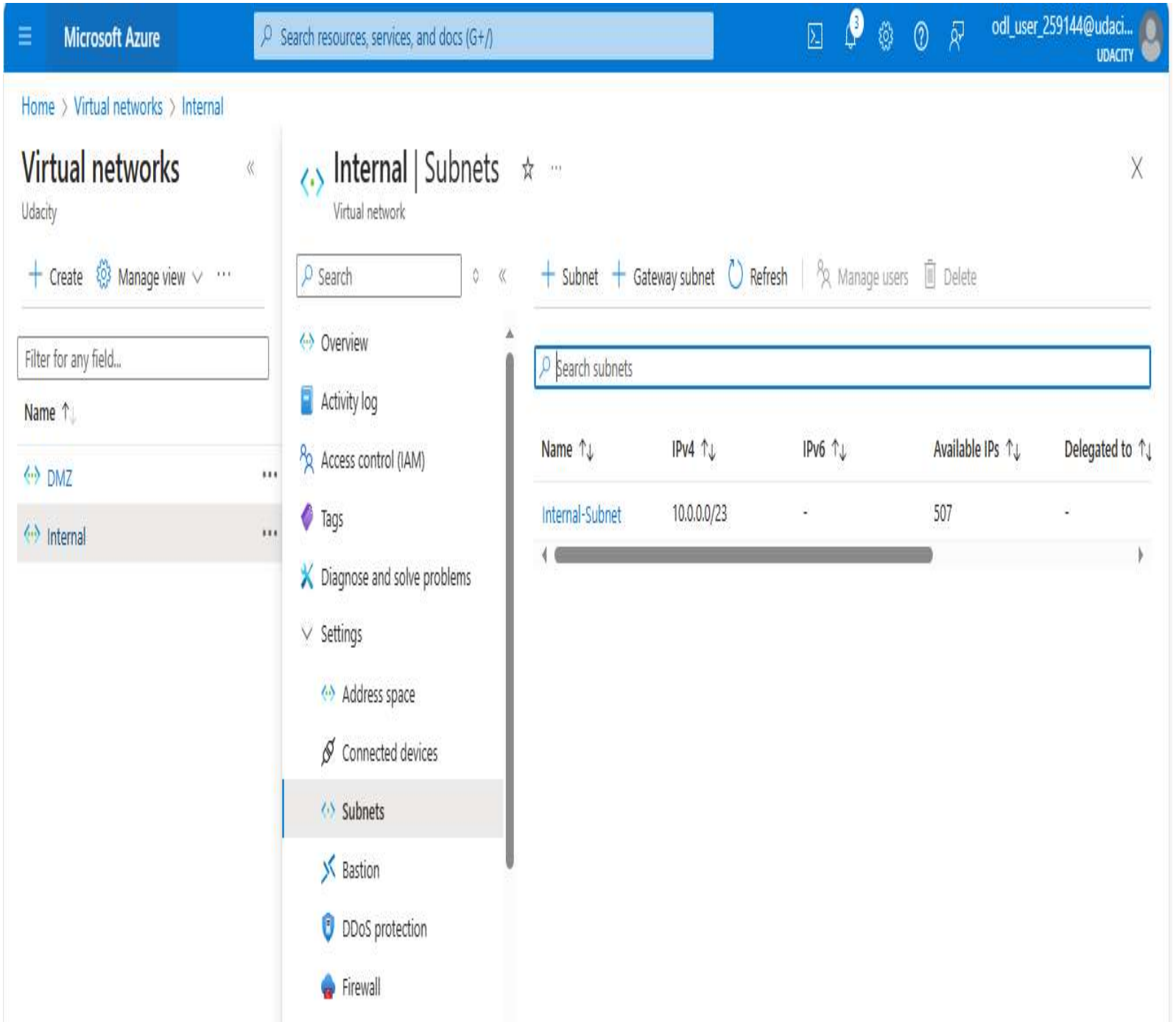
Network Setup

Screenshot of the DMZ Virtual Network with the two subnets



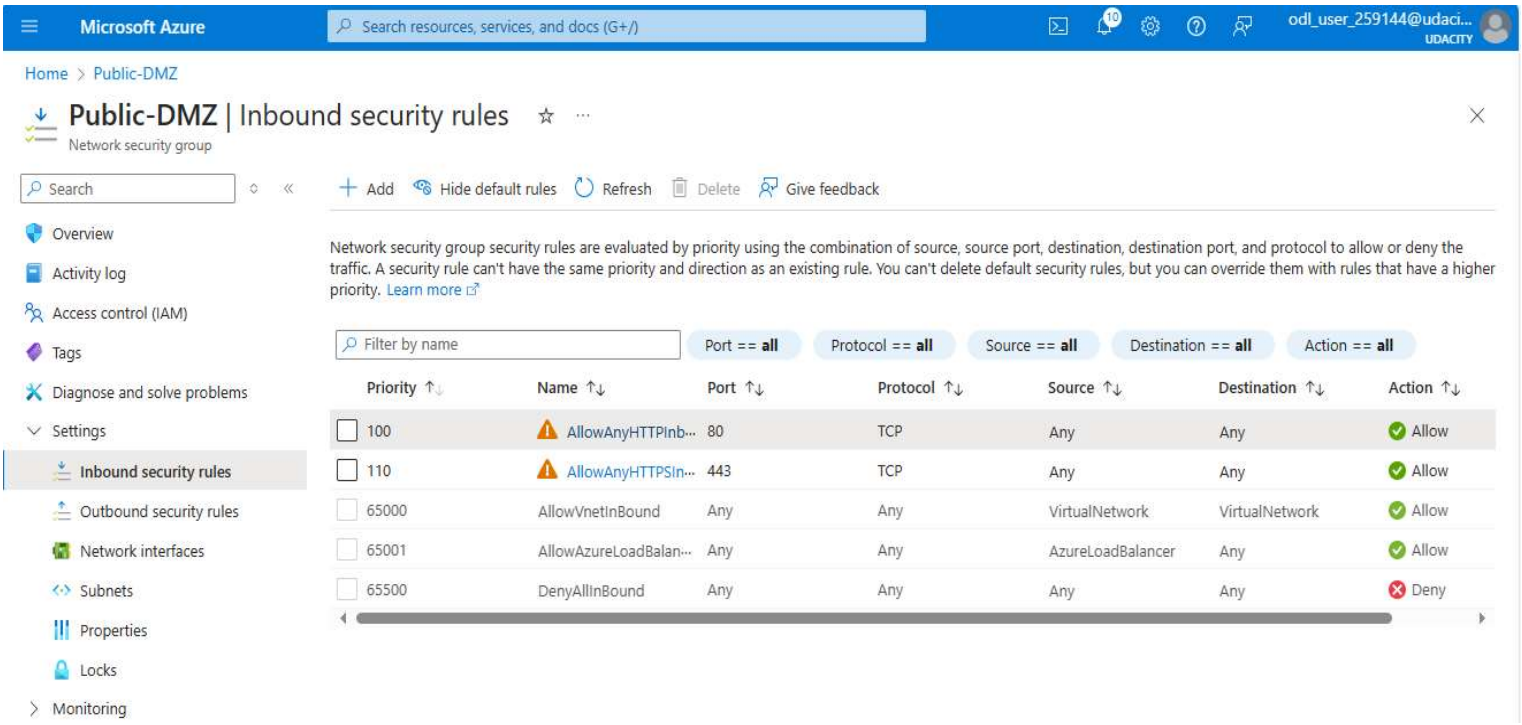
Network Setup

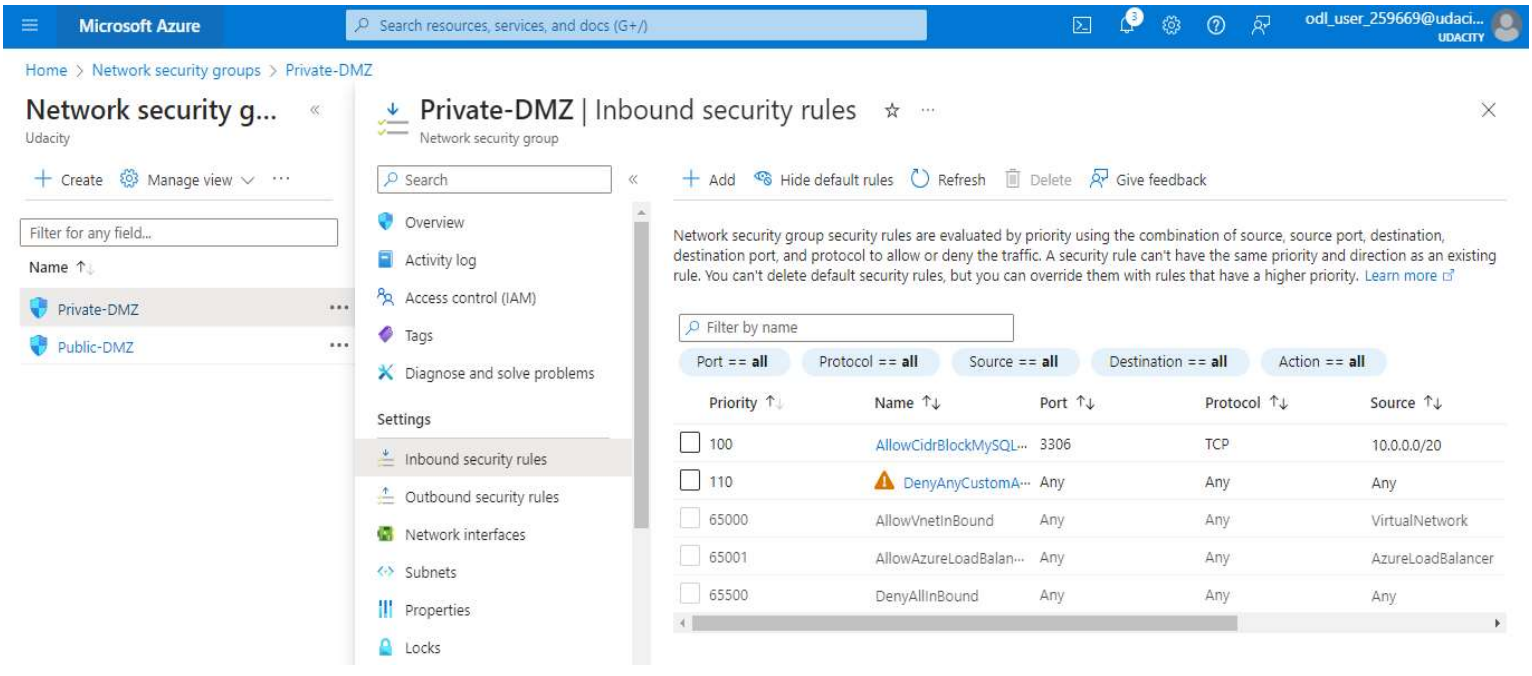
Screenshot of the Internal Virtual Network with the subnet



Secure Routing Setup

Screenshot of the security rules for each subnet.





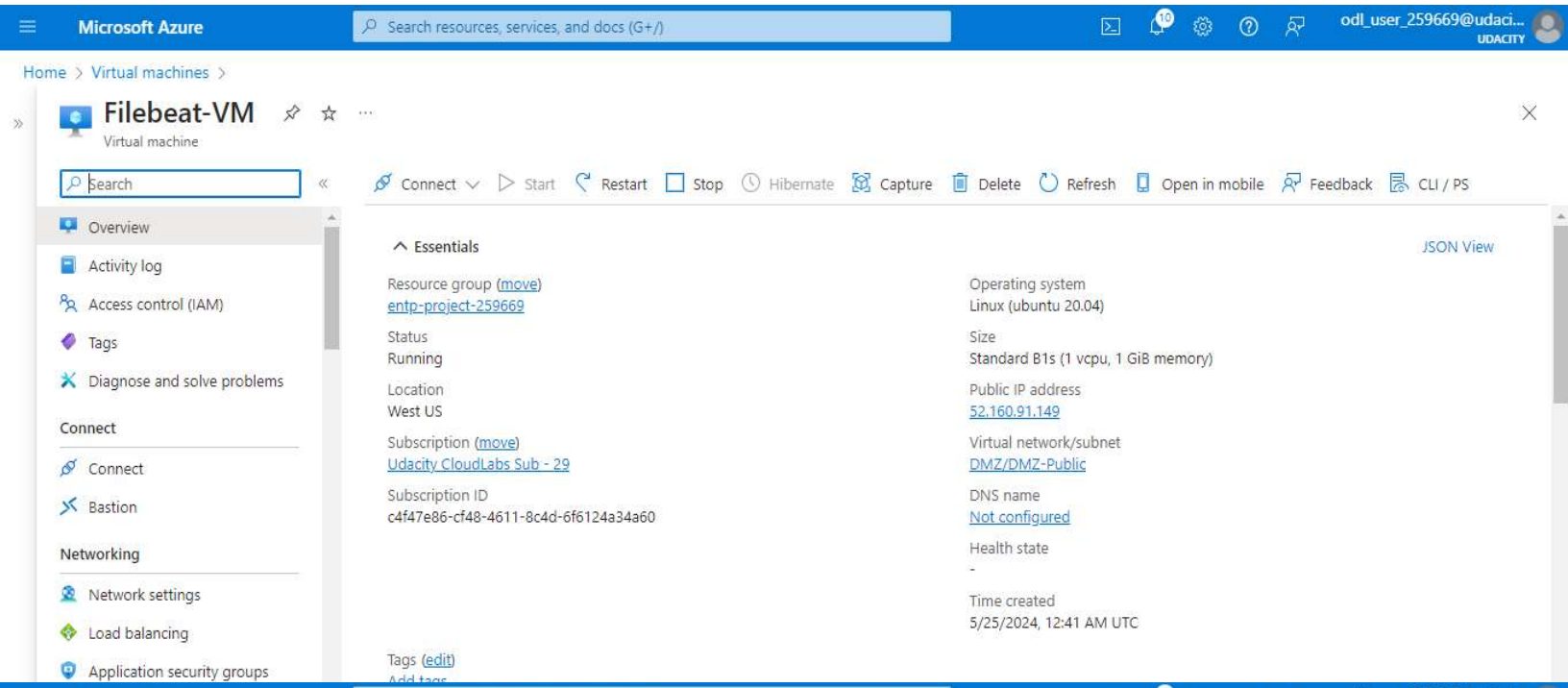
Section Three: Continuous Monitoring with a SIEM

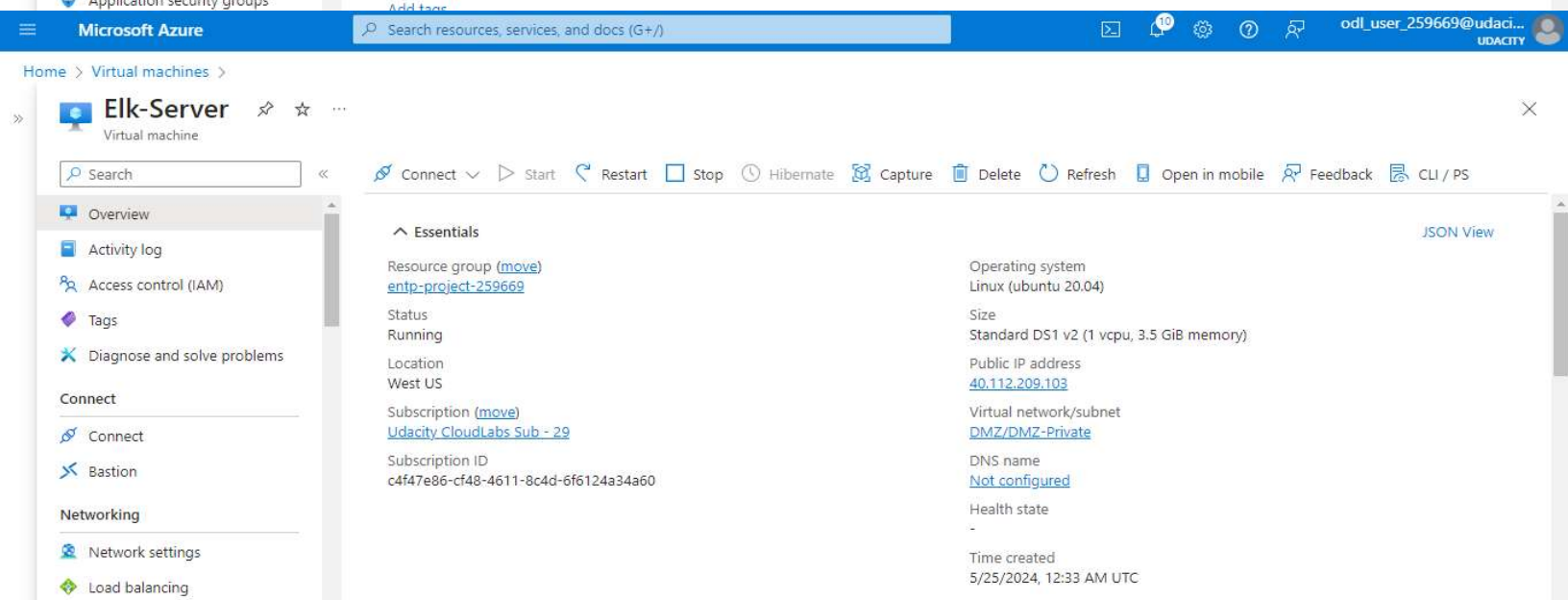
Understanding SIEM Benefits

1. Enhanced Cybersecurity and Fraud Detection:
A SIEM system can help our company quickly detect and respond to suspicious activities, such as unauthorized access attempts, anomalous user behavior, and potential fraud patterns. By identifying these threats in real-time, the SIEM can enable our security team to take immediate action, minimizing the risk of financial losses, data breaches, and reputational damage.
2. Regulatory Compliance and Audit Readiness:
Cryptocurrency exchanges are subject to strict regulatory requirements, such as AML (Anti-Money Laundering) and KYC (Know Your Customer) regulations. A SIEM system can automate the collection, storage, and reporting of security-related data, ensuring our company can easily demonstrate its compliance with these regulations during audits. This not only helps our company avoid costly fines and legal consequences but also builds trust with regulators, customers, and industry partners.
3. Improved Operational Efficiency and Forensic Capabilities:
The SIEM system can centralize and correlate security data from various sources, including network devices, servers, and security tools, providing our security team with a comprehensive view of our company's security posture. This enhanced visibility can lead to more efficient incident investigation, root cause analysis, and forensic capabilities, enabling our team to quickly identify the source and extent of any security incidents or breaches.

Deploy SIEM Components in Azure

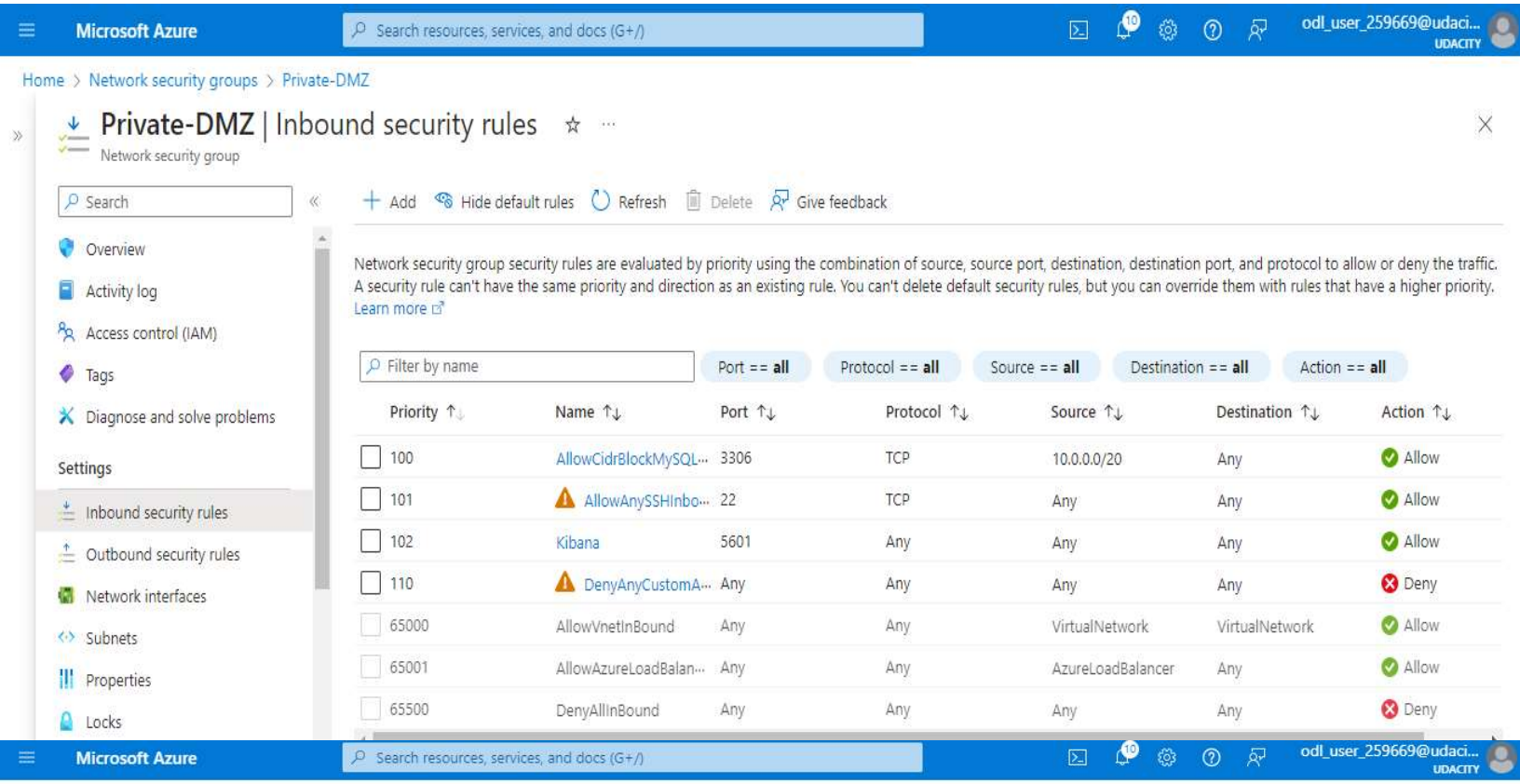
Screenshots of the VM instances confirming their creation and network placement.

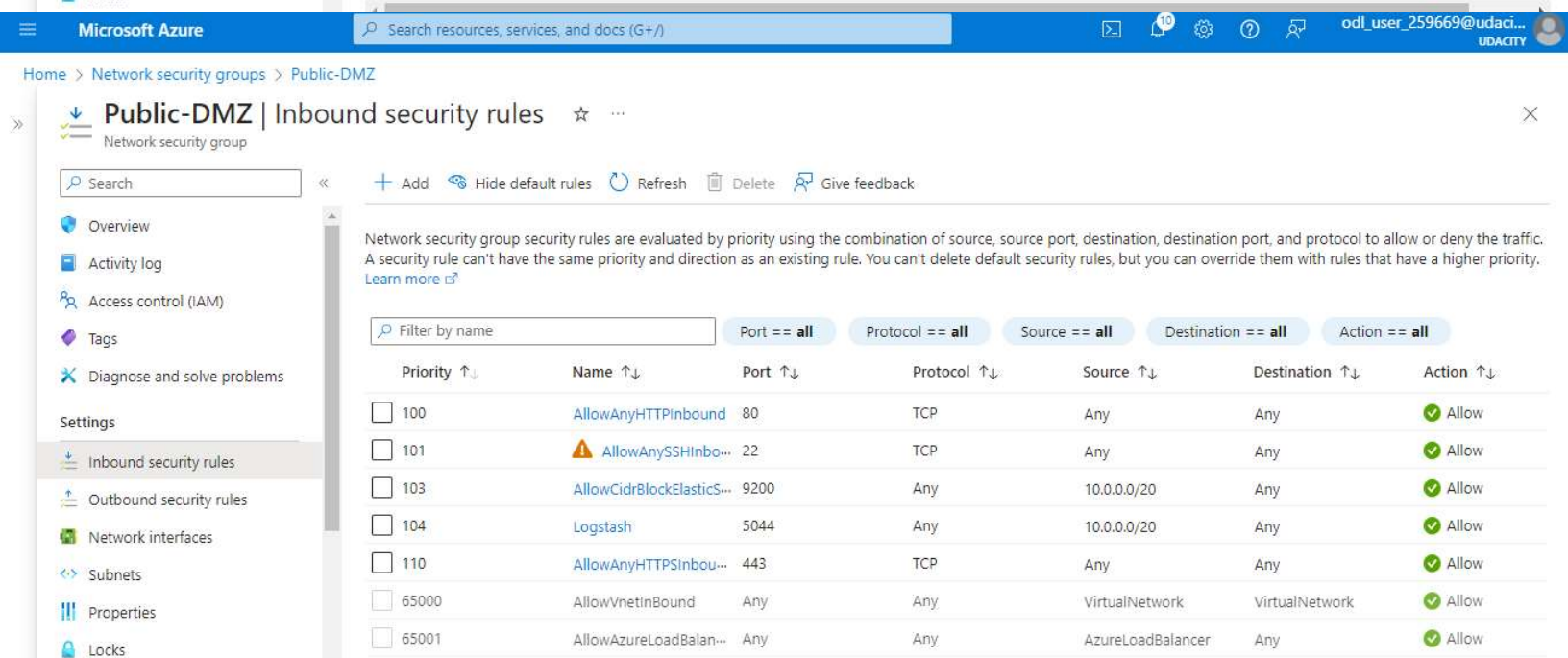




Update the Security Rules

Screenshot of the updated Private-DMZ network security group rules





Setup Monitoring

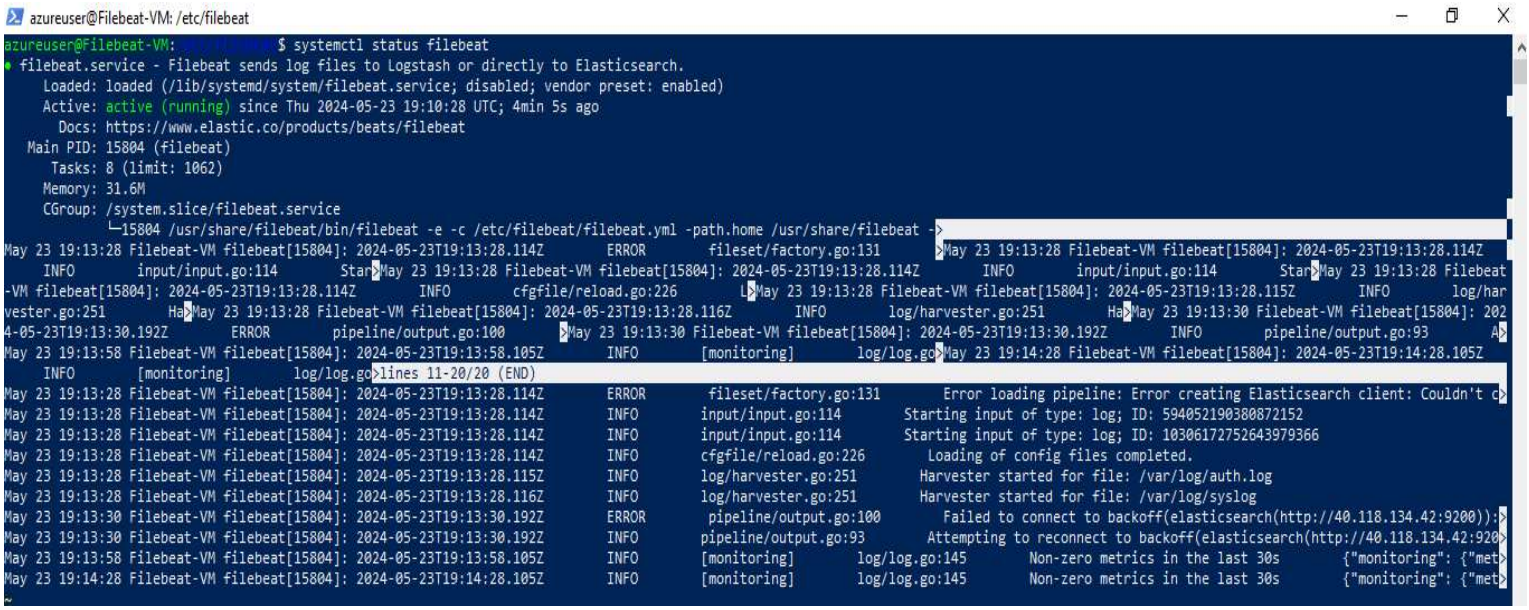
To fully showcase our SIEM's capabilities, we will set up the ELK (Elasticsearch, Logstash, Kibana) server, install Filebeat on our web server, and ensure that web server logs are correctly forwarded and displayed in Kibana. This comprehensive task is pivotal for demonstrating effective real-time monitoring and analysis of web server activity, which is essential for maintaining operational health and security within our infrastructure.

- *Install and configure the ELK server on a VM within the Private-DMZ subnet.*
- *Install Filebeat on the web server in the Public-DMZ subnet.*
- *Configure Filebeat to forward logs to the ELK server's Elasticsearch.*
- *Generate traffic on the web server to create log data (i.e. access the server).*
- *Verify logs are forwarded to Elasticsearch and visible in Kibana.*
- *Create screenshots to confirm that the services are running:*
    - *Filebeat service running on the web server*
        - *Make it from the CLI, with the 'systemctl status filebeat'*
    - *Kibana receives logs from the Filebeat host*
        - *From Kibana site SIEM/Hosts/Filebeat-VM*

Setup Monitoring

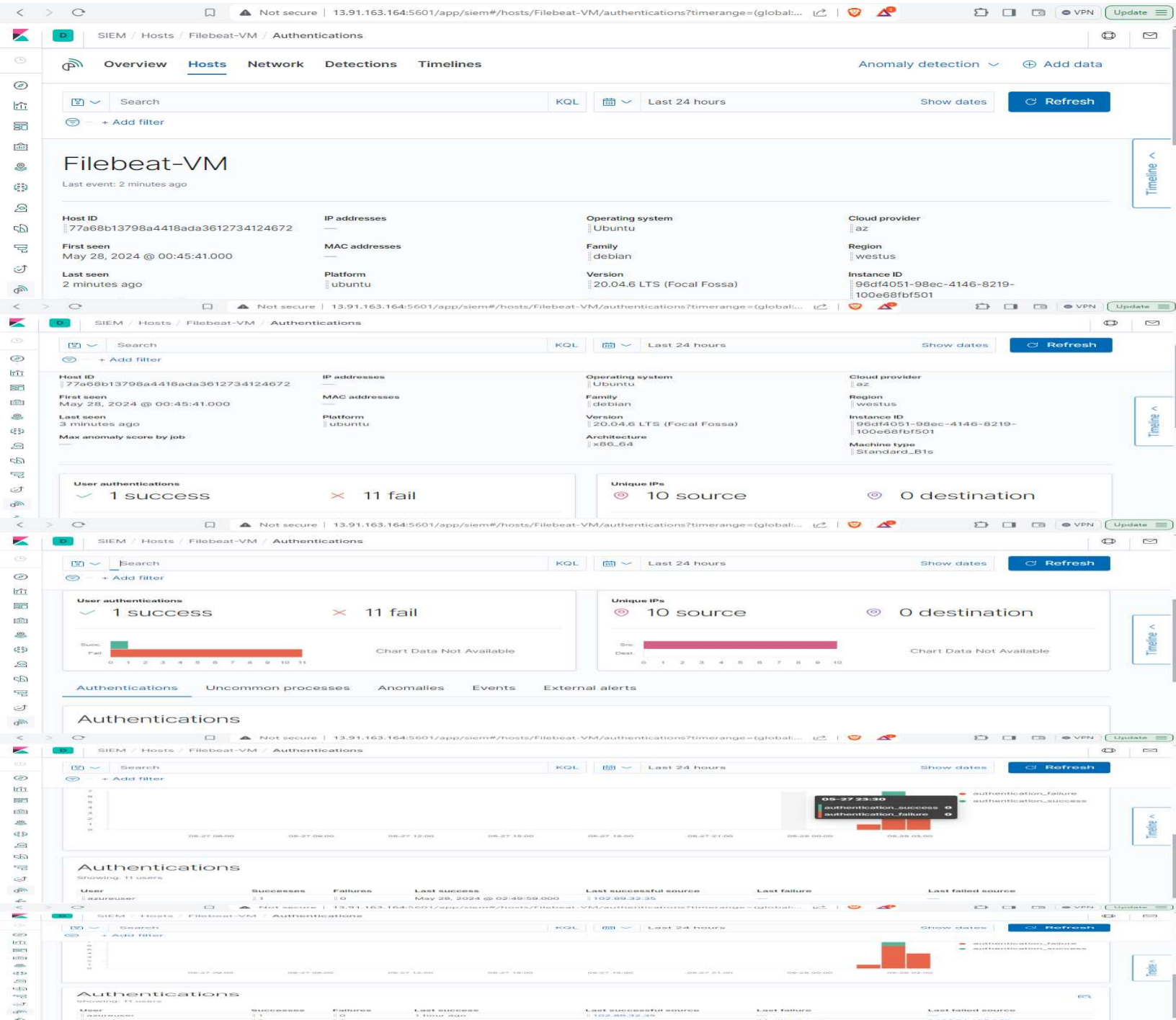
Screenshot of the Filebeat service on the web server (command: 'systemctl status filebeat')

.



Setup Monitoring

Screenshot showing that Kibana receives logs from the Filebeat host (SIEM/Hosts/Filebeat-VM)



Section Four: Zero Trust

Zero Trust Comparison

1. Consideration of all resources	
Zero Trust Approach: considers every device, software, and system as a potential security risk, requiring continuous verification and risk assessment.	**Traditional Approach:** focuses on securing the perimeter, with the assumption that everything inside is trusted.
Benefits of Zero Trust: Reduces the risk of compromised internal assets, as the network assumes no implicit trust, leading to a more proactive and comprehensive security stance.	

2. Secured communication	
Zero Trust Approach: Encrypts all data transfers, regardless of location, ensuring secure communication across the entire network.	**Traditional Approach:** Relies on securing the network perimeter, with the assumption that internal communications are inherently trusted.
Benefits of Zero Trust: Mitigates the risk of data breaches and unauthorized access, even in the event of a perimeter breach, by maintaining end-to-end encryption.	

Zero Trust Comparison

3. Per-session access	
Zero Trust Approach: Grants access to resources only for the duration of a session, requiring continuous re-authentication and access verification.	**Traditional Approach:** Grants access to resources based on user or device identity, with the assumption that access persists until revoked.
Benefits of Zero Trust: Reduces the risk of unauthorized access and privilege escalation, as access is constantly validated and revoked when the session ends, limiting the window of exposure.	

The Zero Trust Model

Enclave Gateway Model
Enclave Gateway: The Ideal Zero Trust Model for XYZ Key Reasons: • Granular Access Control: I. Isolated enclaves for critical resources. II. Tailored access policies for each enclave. • Adaptive Access Policies: I. Consider user, device, and risk factors. II. Responsive to evolving threat landscape. • Centralized Management and Monitoring: I. Comprehensive visibility and control. II. Improved threat detection and response. Aligns with our security objectives: I. Limit resource exposure after breach. II. Enhance network segmentation and resilience. III. Adopt a proactive, context-aware security approach. The Enclave Gateway model best addresses our current security challenges and supports our transition to a robust Zero Trust architecture.