UDACITY

Securing the Perimeter

Uriyah Adriel Sam

16-05-2024

Digital Project Management

Project Scenario

Digital Project Management Section One:

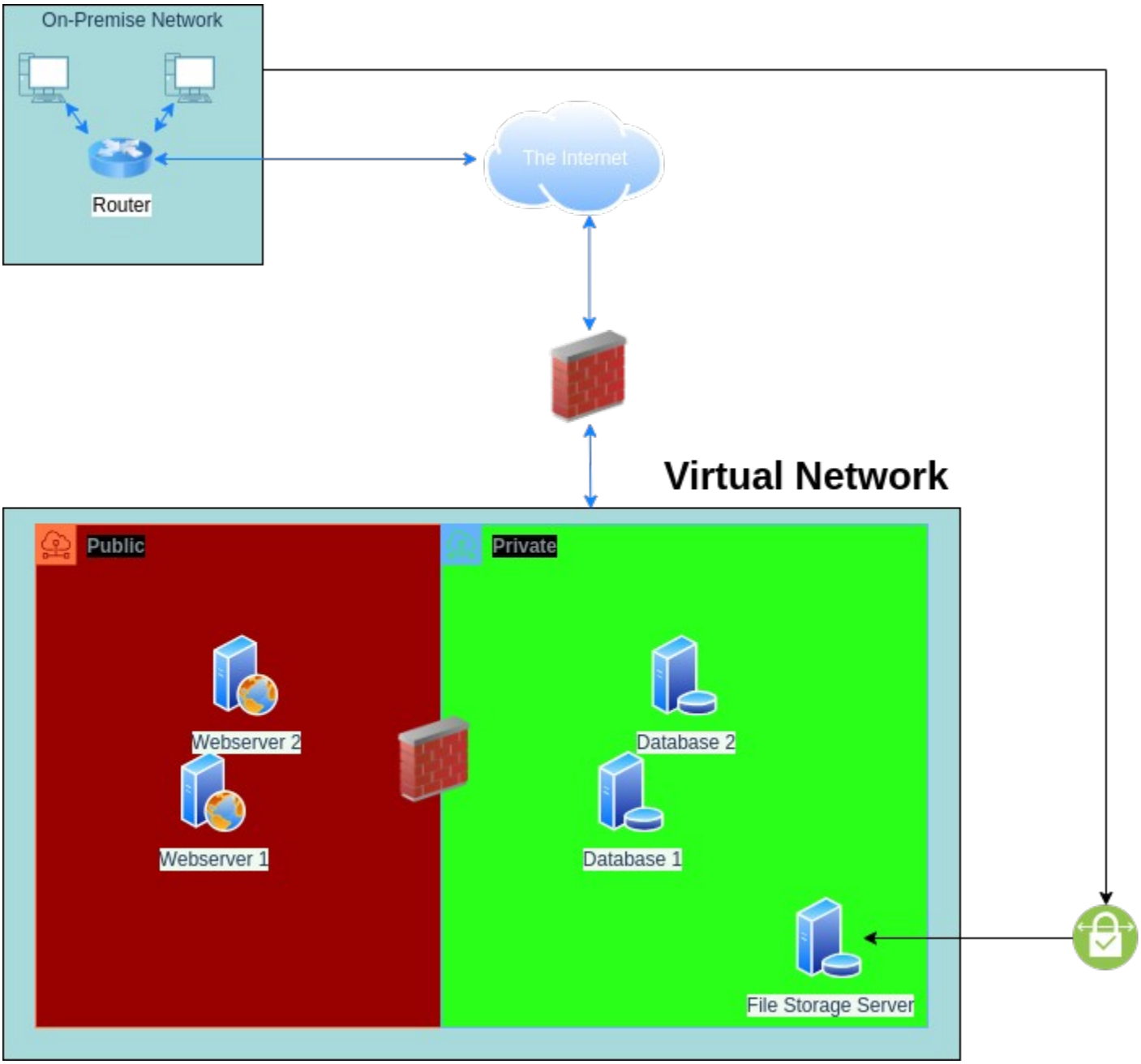
Designing a Secure Network Architecture

Identify Network Vulnerabilities

1. Lack of Segmentation
The current setup places all servers within a single virtual network and subnet, lacking proper segmentation. This means that if one server is compromised, the entire network could be at risk. For instance, if one of the web servers were to be breached, the attacker would have easy access to the database servers as they are on the same network segment. This increases the potential damage that can be caused by an attacker and makes lateral movement within the network easier.
2. Direct Internet Connections for All Servers
All servers having direct connections to the internet without proper firewall or security measures is a significant security concern. This setup exposes the servers to a higher risk of unauthorized access, malware infections, and other cyber threats. For example, without adequate firewall protection, the servers are vulnerable to various types of attacks such as DDoS, brute force attacks, and exploits targeting specific services or vulnerabilities.
3. Lack of Access Control for File Storage Server
The file storage server being accessible from the on-premise network without proper access controls poses a significant security risk. Without proper authentication and authorization mechanisms in place, there's a risk of unauthorized access to sensitive data stored on the file server. For instance, if an attacker gains access to the on-premise network, they could potentially exploit this vulnerability to gain unrestricted access to the file storage server and exfiltrate sensitive data or deploy malicious software.

Network Redesign

Place the updated network diagram here.



Identify Network Vulnerabilities

Why do we need to add firewalls to our network?

Adding firewalls to our network is essential for enhancing security by enforcing access control and filtering traffic. Firewalls act as a barrier between our internal network and external threats, such as unauthorized access attempts and malicious traffic from the internet. By carefully configuring firewall rules, we can restrict access to specific services and resources, ensuring that only authorized users and traffic are allowed into our network. This helps prevent potential security breaches and protects sensitive data from unauthorized access or compromise.

What is the benefit of having different areas in our network for web servers and database servers?

Segregating our network into different areas, such as separating web servers from database servers, provides several security benefits. Firstly, it reduces the risk of unauthorized access to sensitive data by isolating critical resources like databases from public-facing services like web servers. This limits the attack surface and mitigates the impact of potential security breaches. Additionally, it allows us to implement granular access controls and security policies tailored to the specific requirements of each area, ensuring that only necessary and authorized communication is allowed between them. Overall, this segmentation enhances security and control over network traffic, minimizing the risk of security incidents and data breaches.

What does a VPN do for our connection to the file storage server?

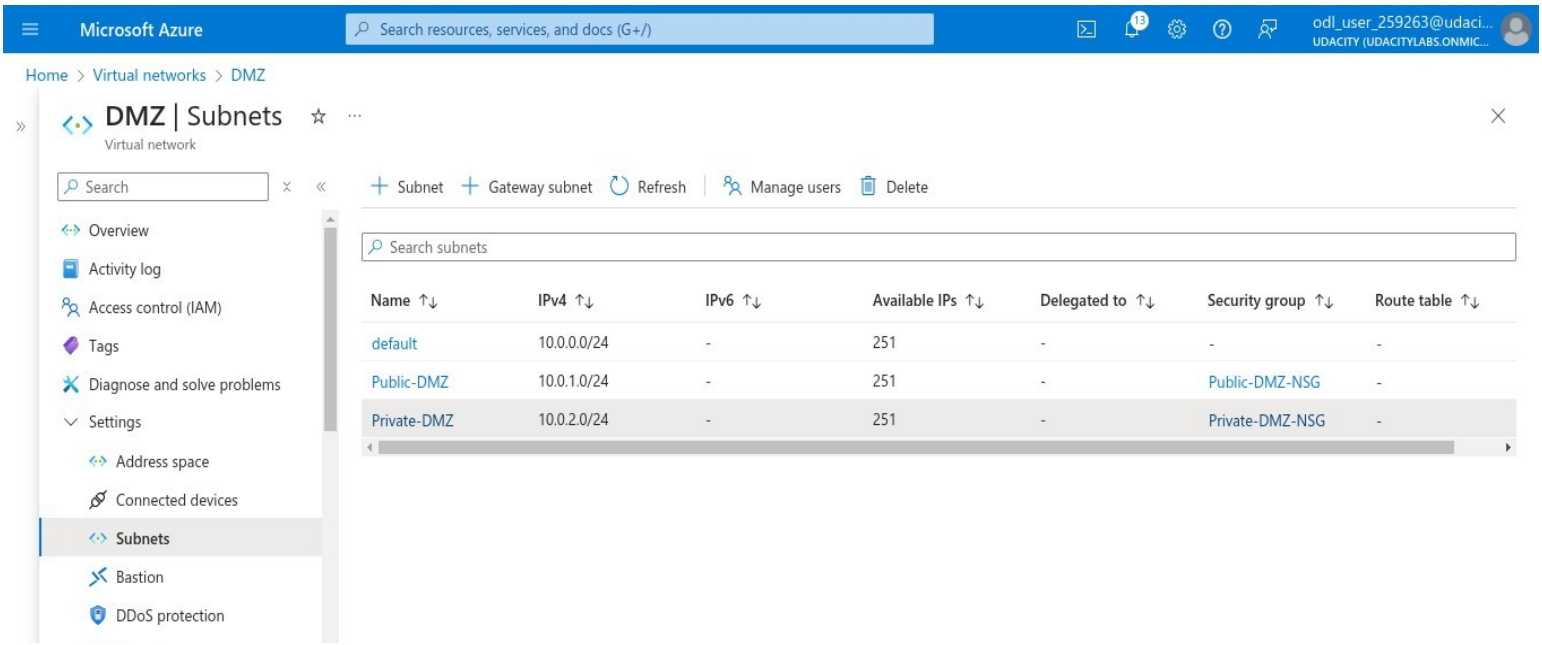
Implementing a Virtual Private Network (VPN) for our connection to the file storage server offers several security benefits. A VPN establishes a secure, encrypted tunnel between our on-premise network and the file storage server in the virtual network, ensuring confidentiality and integrity of data transmission. This means that data exchanged between our network and the file storage server is protected from interception and tampering by unauthorized parties. By leveraging VPN technology, we can securely access and transfer sensitive files and information between our on-premise infrastructure and the file storage server, safeguarding our data assets from potential security threats and unauthorized access.

Digital Project Management

Section Two: Building a Secure Network Architecture in Azure

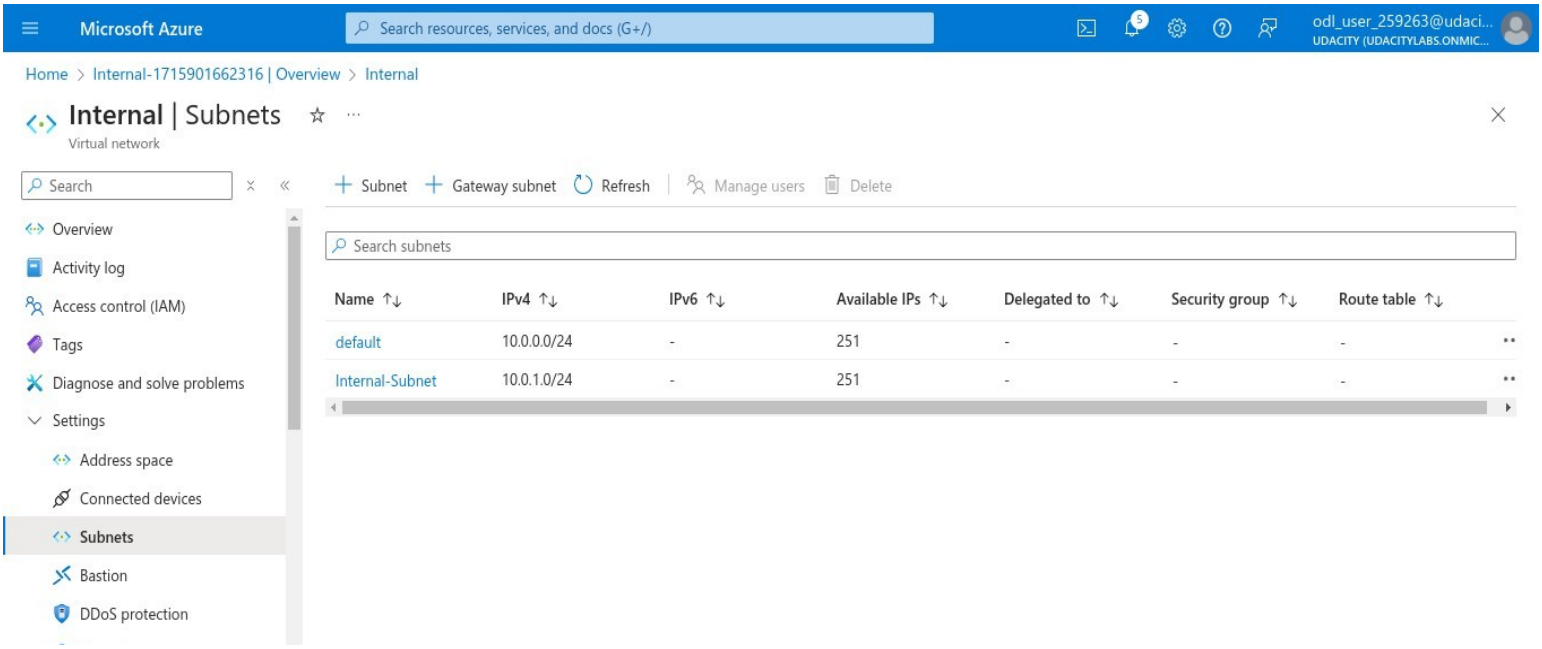
Network Setup

Screenshot of the DMZ Virtual Network with the two subnets

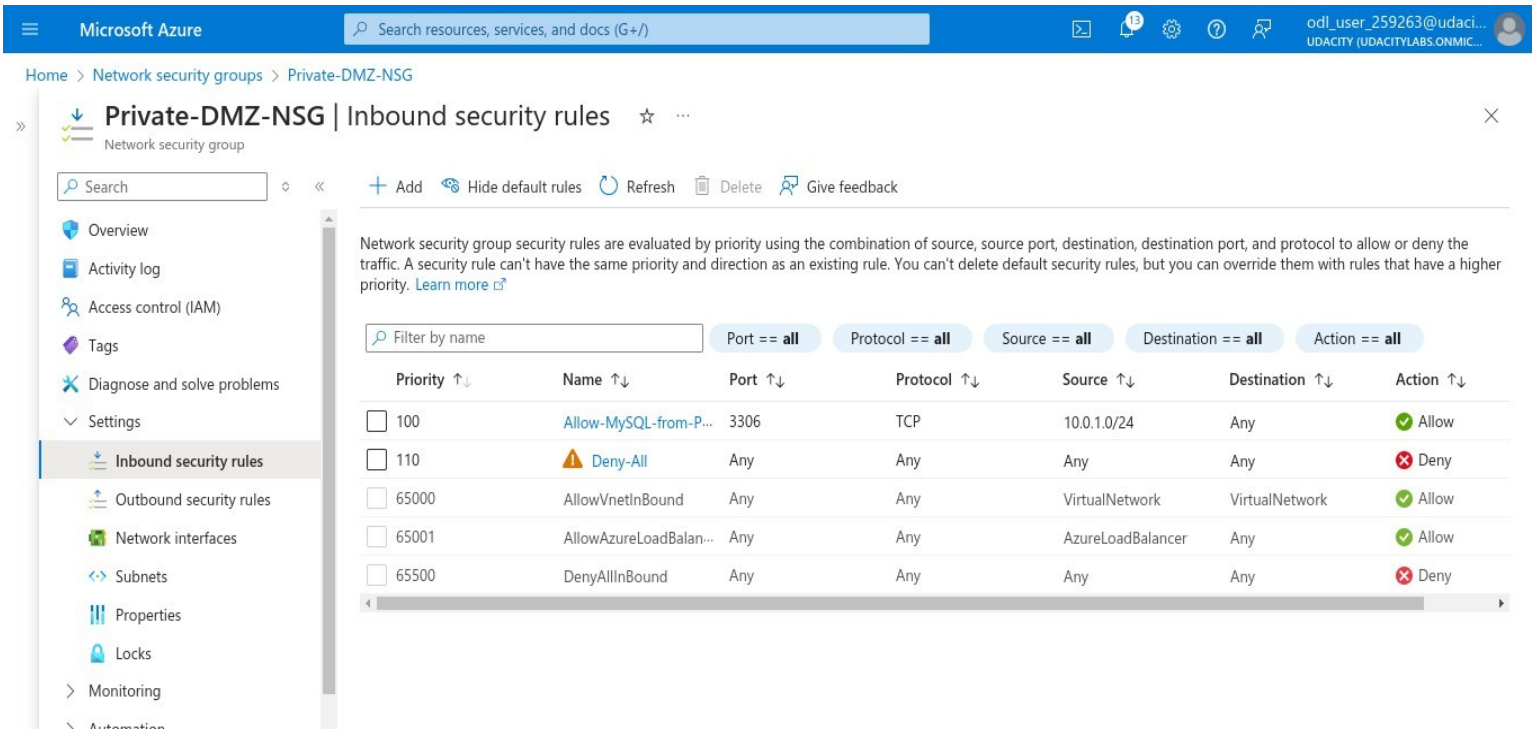


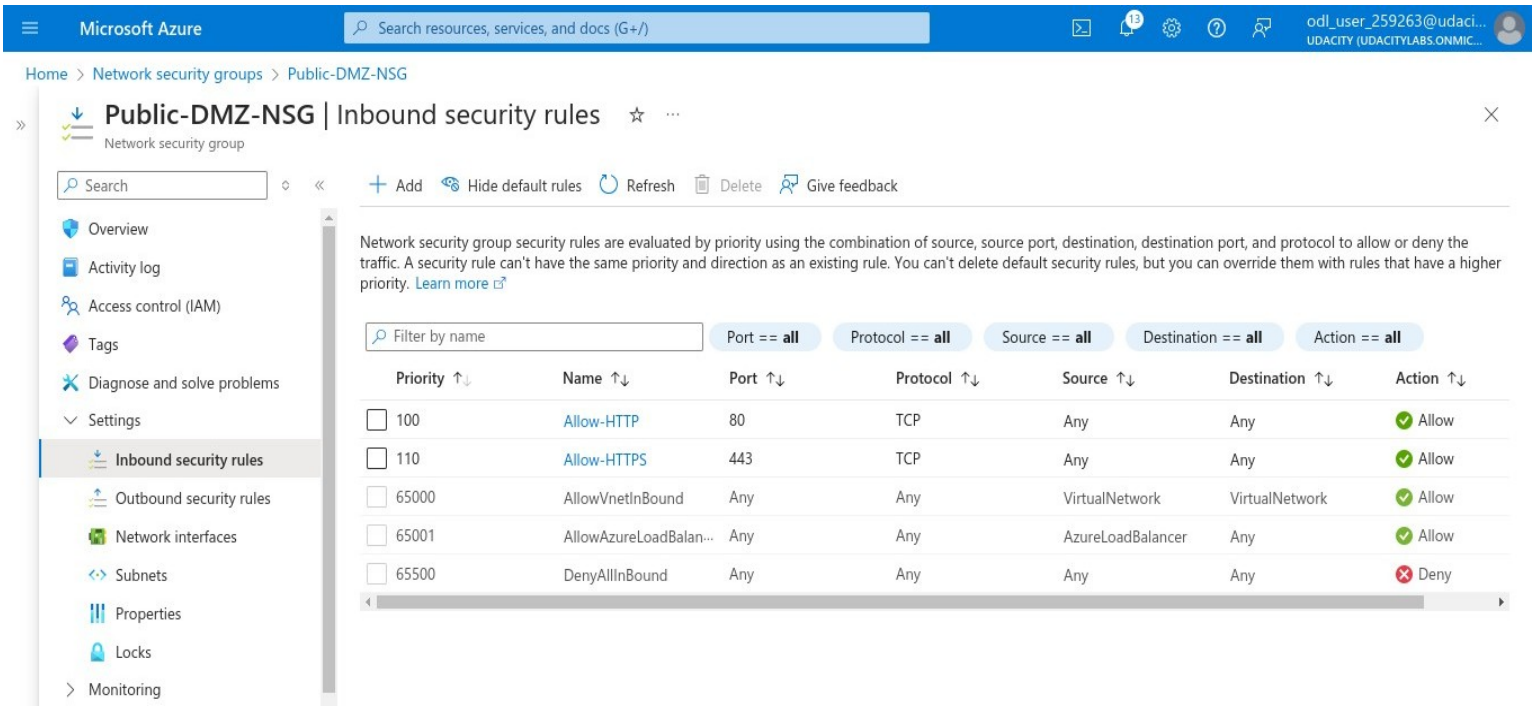
Network Setup

Screenshot of the Internal Virtual Network with the subnet



Secure Routing Setup





Digital Project Management

Section Three: Continuous Monitoring with a SIEM

Understanding SIEM Benefits

1. Enhanced Threat Detection and Response

- SIEM systems aggregate and analyze security data from various sources, such as network devices, servers, applications, and logs, in real-time.
- By correlating events and identifying patterns indicative of security threats, SIEM enables early detection of potential cyber threats, including malware infections, suspicious user activities, and unauthorized access attempts.
- Rapid detection of security incidents allows organizations to respond promptly, mitigating the impact of breaches and minimizing downtime, data loss, and financial losses.

2. Improved Compliance and Regulatory Compliance

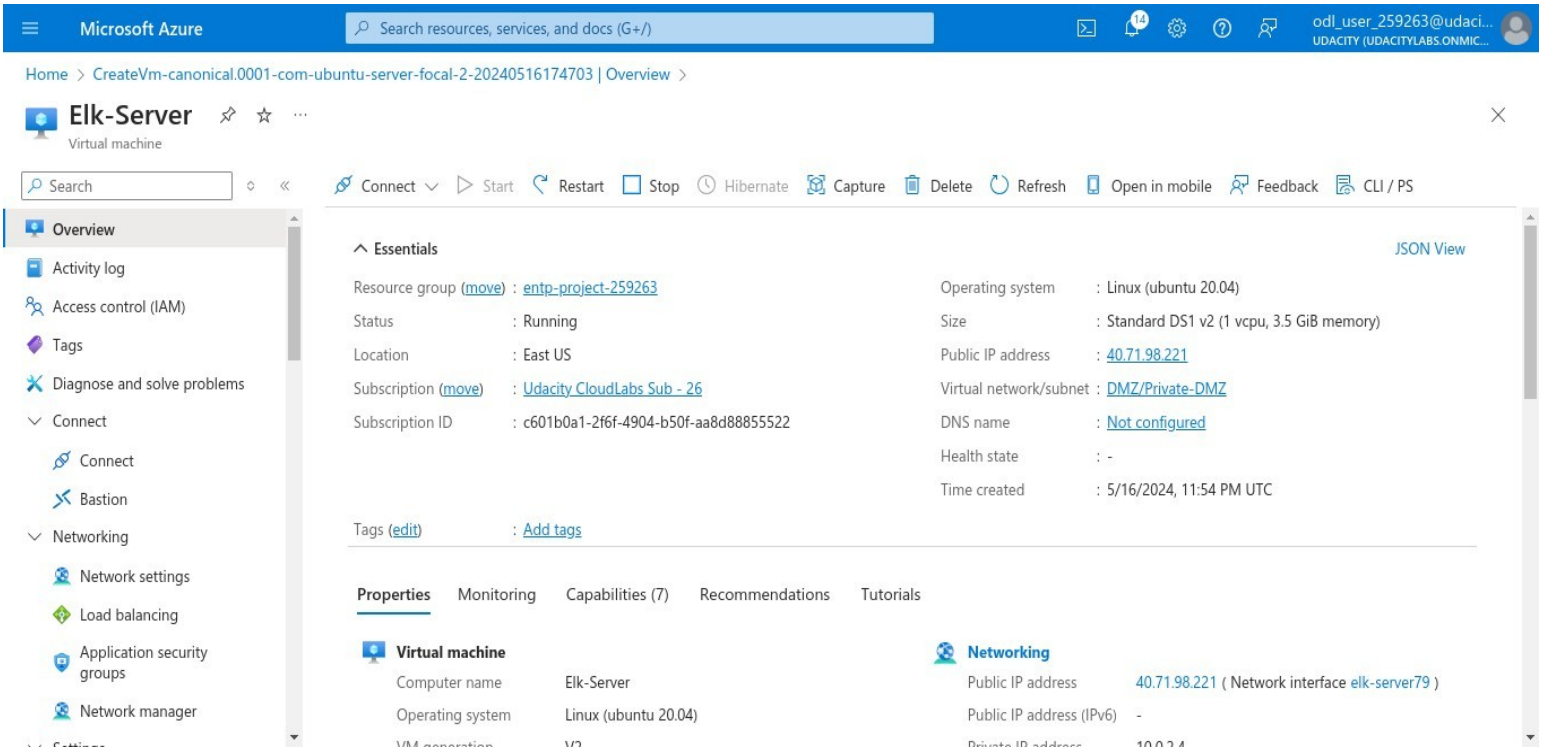
- SIEM solutions help organizations meet compliance requirements mandated by industry regulations and data protection laws, such as GDPR, HIPAA, PCI DSS, and SOX.
- By centralizing log management and providing comprehensive audit trails and reporting capabilities, SIEM systems facilitate compliance monitoring, reporting, and documentation.
- Automated compliance checks and alerting mechanisms ensure timely identification of non-compliant activities, helping organizations avoid penalties, fines, and reputational damage associated with regulatory violations.

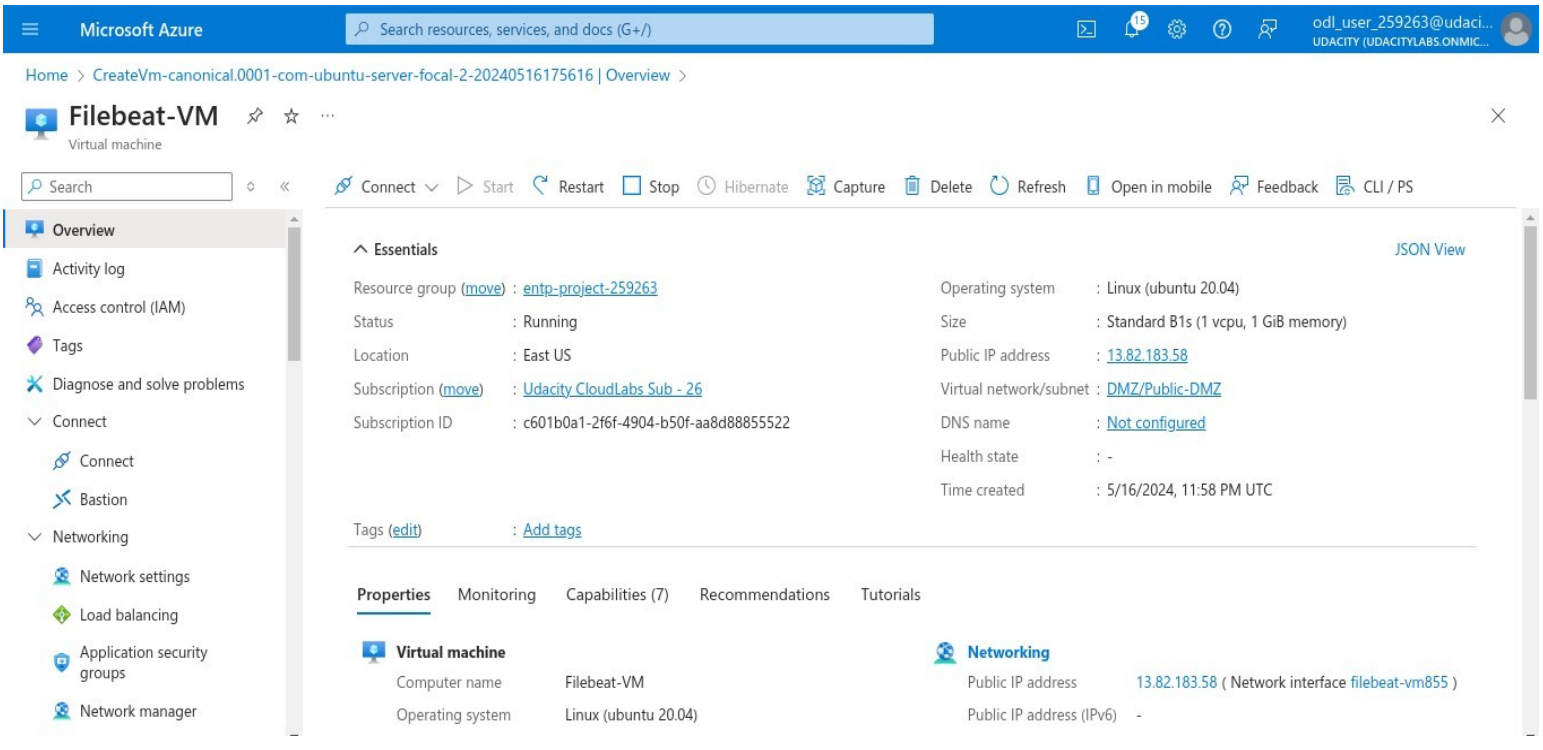
3. Effective Security Incident Investigation and Forensics

- SIEM platforms provide robust investigation and forensic capabilities, allowing security teams to analyze security incidents, conduct root cause analysis, and track the timeline of events.
- Advanced search functionalities and customizable dashboards enable security analysts to quickly identify and analyze relevant security events, reducing investigation time and effort.
- Historical data retention and forensic analysis capabilities facilitate post-incident analysis, enabling organizations to learn from security incidents, strengthen defenses, and improve incident response processes over time.

Deploy SIEM Components in Azure

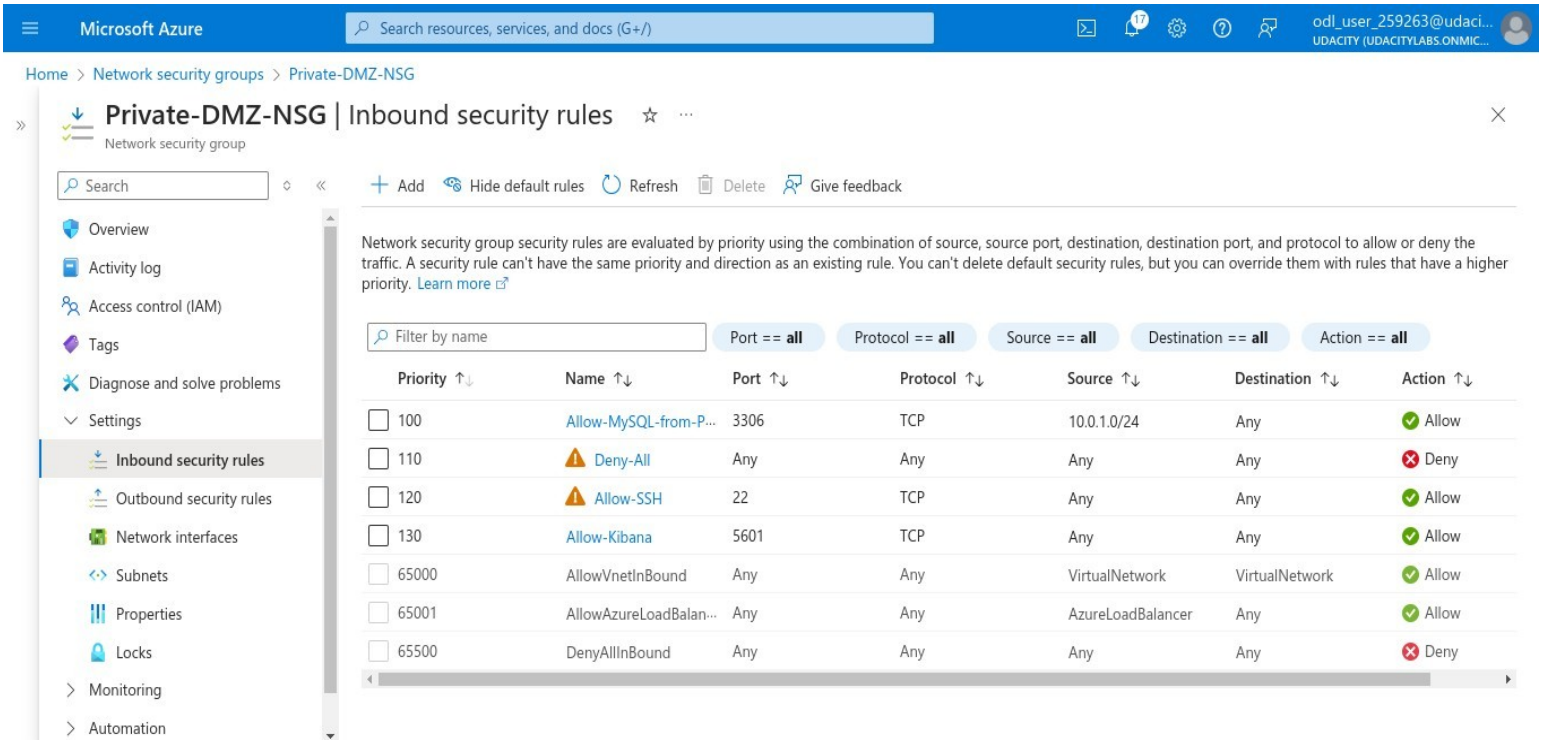
Screenshots of the VM instances confirming their creation and





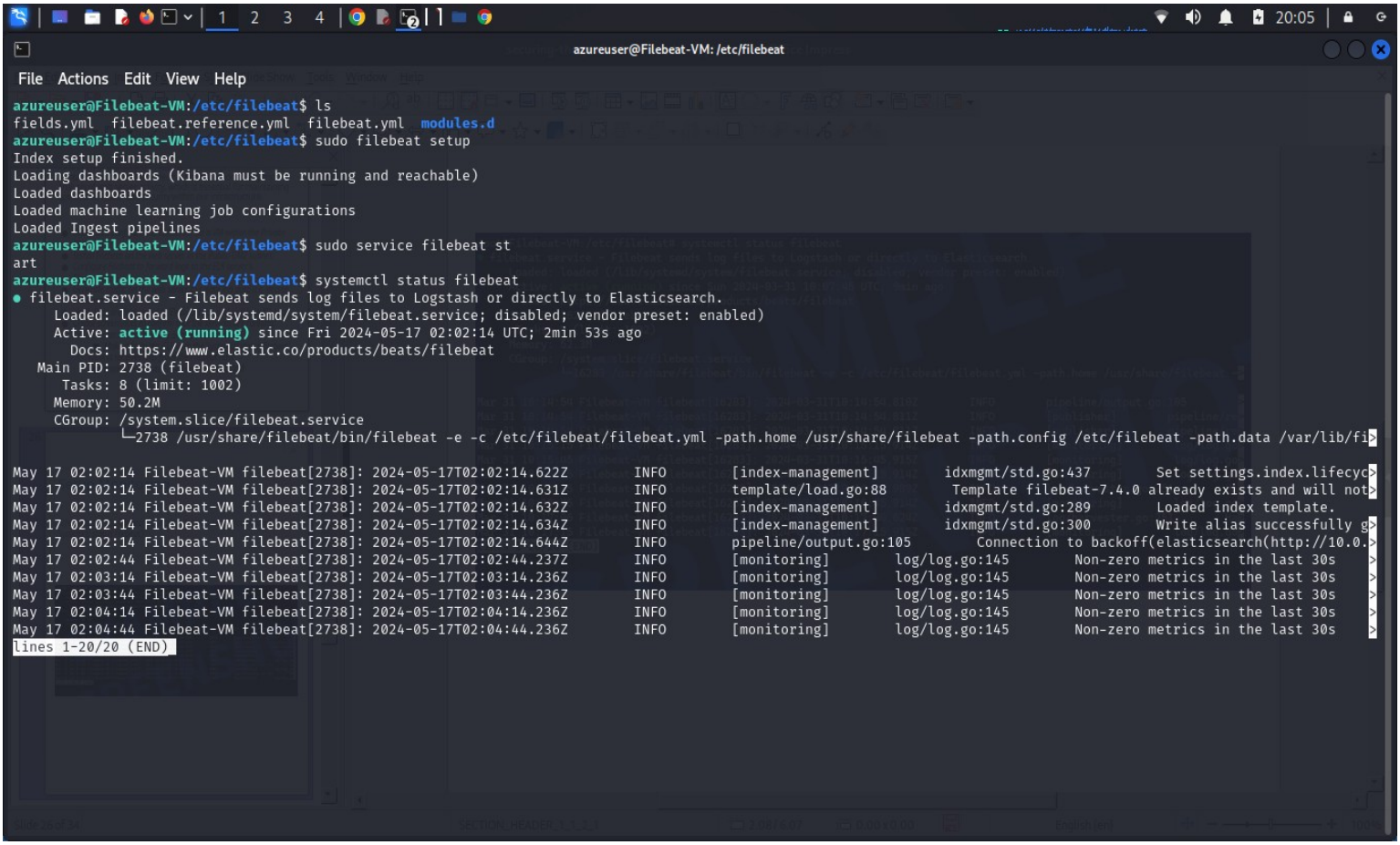
Update the Security Rules

Screenshot of the updated Private-DMZ network security group rules



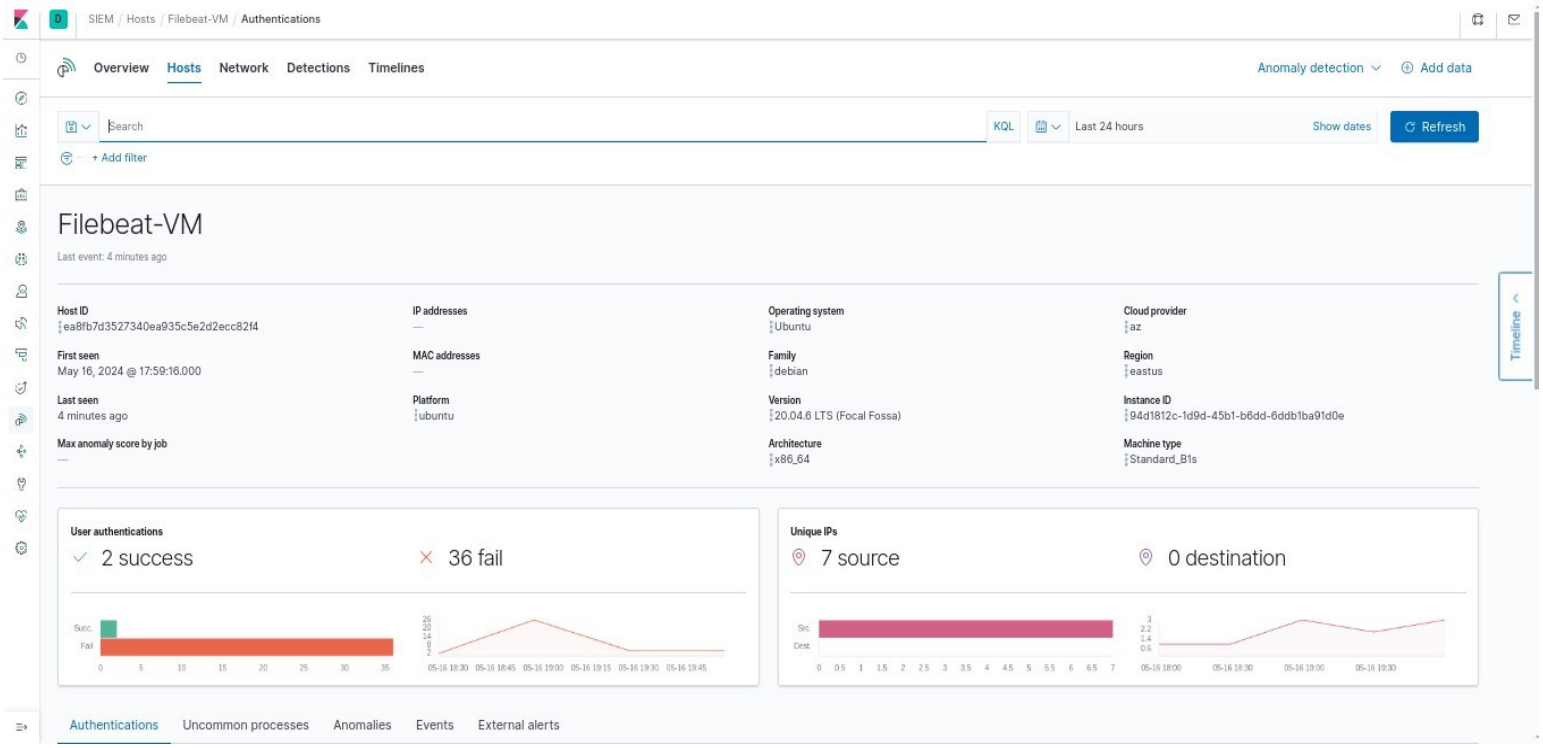
Setup Monitoring

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)



Digital Project Management

Section Four: Zero Trust

Zero Trust Comparison

1. Secured communication: Encrypt all data transfers, irrespective of location	
Zero Trust Approach: In a Zero Trust architecture, all data transfers are encrypted, regardless of where the communication is occurring within the network. This ensures that even if an attacker gains access to the network, they cannot eavesdrop on sensitive information.	**Traditional Approach:** In traditional network security models, encryption might be applied selectively, typically only for communication over external networks or between certain critical systems. Internal communication within the network may not be encrypted, leaving data vulnerable to interception by attackers who gain unauthorized access.
Benefits of Zero Trust: By encrypting all data transfers, Zero Trust ensures that data remains protected even if an attacker gains a foothold within the network. This proactive security measure significantly reduces the risk of data breaches and unauthorized access.	

Zero Trust Comparison

2. Dynamic access policy: Access is based on real-time evaluations of multiple factors	
Zero Trust Approach: Zero Trust architecture dynamically evaluates multiple factors, such as user identity, device health, location, and behavior, before granting access to resources. Access decisions are made in real-time based on the current context, reducing the attack surface and mitigating the risk of unauthorized access.	**Traditional Approach:** In traditional network security models, access control policies are often static and based on predefined rules or roles. Once access is granted, it remains unchanged until manually modified, regardless of changes in user behavior or environmental factors.
Benefits of Zero Trust: Dynamic access policies in Zero Trust architecture enhance security by continuously adapting access controls based on the current context. This proactive approach reduces the likelihood of unauthorized access and minimizes the impact of security breaches by limiting attackers' ability to move laterally within the network.	

Zero Trust Comparison

3. Continuous monitoring: Real-time assessment of asset integrity and security.	
Zero Trust Approach: Zero Trust architecture incorporates continuous monitoring mechanisms to assess asset integrity and security in real-time. This involves monitoring network traffic, user behavior, device health, and other relevant factors to detect and respond to potential security threats promptly.	**Traditional Approach:** Traditional network security models often rely on periodic security assessments, such as vulnerability scans or manual audits, to evaluate asset integrity and security. These assessments may occur at predetermined intervals and may not provide real-time insights into emerging security threats.
Benefits of Zero Trust: Continuous monitoring in Zero Trust architecture enables organizations to detect and respond to security threats proactively. By continuously monitoring network activity and user behavior, organizations can identify anomalous behavior and potential security incidents more quickly, minimizing the impact of cyberattacks and reducing the risk of data breaches.	

The Zero Trust Model

Device Agent & Gateway
The Device Agent & Gateway model is the best fit for XYZ due to its comprehensive endpoint security, granular access control, scalability, flexibility, and enhanced visibility. This approach ensures robust protection against recent security vulnerabilities by deploying agents on devices, enforcing stringent access controls, adapting to evolving network environments, and providing real-time monitoring capabilities. It offers XYZ a holistic solution to strengthen their security posture and mitigate the risk of unauthorized access and data breaches.