Securing the Perimeter

Project Scenario

Overview

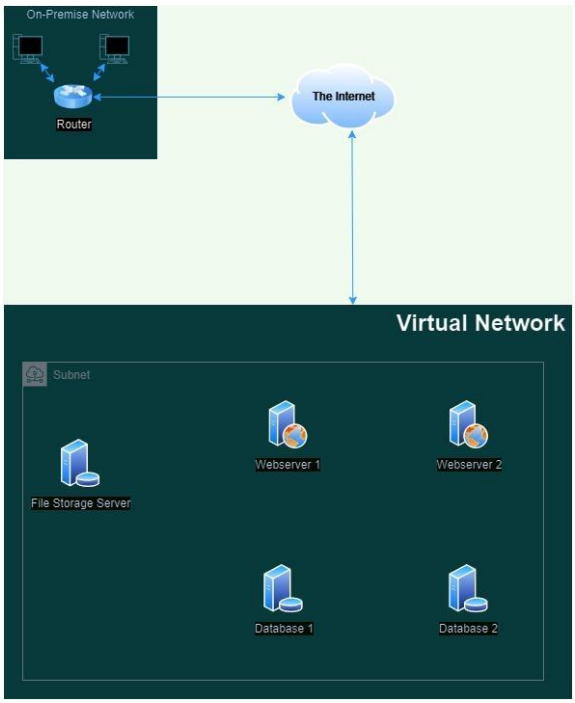
XYZ is the premier cryptocurrency exchange. They transact over a billion trades everyday and are considered to be one of the most reliable and secure exchanges in the world. Due to their rapid growth, they've faced challenges in scaling their security posture.
The largest challenge they've faced is with 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 1: Designing a secure Network Architecture

Network Description



- *The on-premise network is connected to a virtual network through the internet.*
- *All five servers are located within a single virtual network and in one subnet.*
- *All servers have direct connections to the internet.*
- *The two web servers are required to communicate with the two database servers to function correctly.*
- *The file storage server only needs to be accessible from the on-premise network.*

Project Information Slide

Review for the provided network diagram

- Review > *The provided network diagram illustrates a hybrid network architecture combining an on-premise network with a cloud based virtual network environment. Two computers are shown connected with router and forming the primary internal LAN infrastructure.The router maintains a direct connection to the internet, establishing the route for all external communications. The virtual network is accessible through the internet, indicating remote hosted resources. Now the intersting part is all the server are situated in same subnet, where file storage server showes centralized storage solution, likely accessible by both webserver and database. Two webserver showes load-balancing design for high availability and scalability also separated database for redundancy, load distribution. We can see the only separation between physical and logical (on-premise and virtual). The structure is sutiable for scalable web applications requiring high uptime and disaster recovery capabilities.*

- *Recommendations for improvement*

➢ *Security gateways* > *Consider adding explicit firewalls or security appliances at the subnet and internet junction to strengthen perimeter defense.*

➢ *Network segmentation* > *Separate webserver and database into different subnets for enhanced security to restrict direct internet access and database.*

➢ *VPN or dedicated connection* > *For improved privacy and reliability, use VPN or dedicated lines between on-premise and virtual networks.*

Identify Network Vulnerabilities

1. [Insecure network architecture]

[**Description** > As we can see the diagram shows all the servers are located within a single virtual network and in one subnet and directly connect with internet without any protection (like firewall).]
[**Risk** > Without segmentation and protection, critical resources are vulnerable to unauthorized access, exploitation and cyber attacks like brute force,malware injection etc. Attackers could target and potentially compromise sensitive system, leading to data breaches and service disruptions.]

2. [Lack of network segmentation]

[**Description** > All database server, web server, file server located within a single network and subnet.]
[**Risk** > If an attacker gains access to any system (such as a compromised web server), they can move laterlly with ease to sensitive back-end systems like database, file storage. This architecture greatly increases the potential impact of a single breach, enabling threats like ransomware or data exfiltration across the network.]

3. [Missing access controls and monitoring]

[**Description** > There is no indication of access control mechanisms like firewall, VPN, multi-factore authentication or security monitoring solutions like intrusion detection system deployed in the setup.]
[**Risk** > Absence of strict access control exposes all systems to unauthorized or unrestricted inbound and outbound traffic, which could be a cause of cyber attack and data leakage. Without monitoring, security incidents may go undetected, allowing attackers to persist in the network and escalate privileges without timely response.]

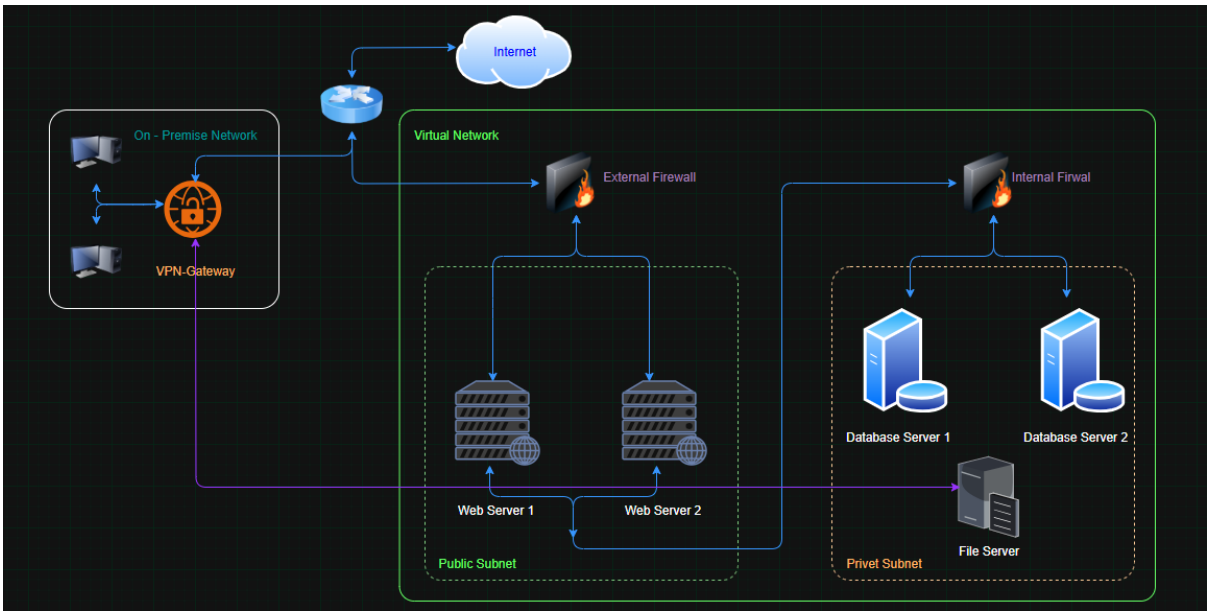
Network Redesign

With the vulnerabilities identified, it’s time to rearchitect the network. A well-structured network with proper security controls is vital for defending the company's digital assets.

- Use drawio.com to create the updated diagram. You can download the original diagram from here.
- *Update the network diagram to include:*
  - *Network segmentation separating public-facing services from internal services.*
  - *Placement of firewalls to control and filter traffic*
  - *A secure, encrypted connection method for the on-premise network to access the file storage server.*
- *Ensure the updated diagram reflects these additions clearly.*

Network Redesign

- *Updated network diagram:*
  - *Network segmentation separating public-facing services from internal services.*
  - *Placement of firewalls to control and filter traffic*
  - *A secure, encrypted connection method for the on-premise network to access the file storage server.*
  - *The file link.*



Convince the Stakeholders

With a proposed network redesign, stakeholders will require a clear understanding of the benefits and necessity of these changes. our next task is to prepare answers to the following potential questions they may have. In all my answers,I try to make sure to emphasize the security aspects.

- Why do we need to add firewalls to our network?
- What is the benefit of having different areas in our network for web servers and database servers?
- What does a VPN do for our connection to the file storage server?

Convince the Stakeholders

Why do we need to add firewalls to our network?

[Firewalls will provide strong securitu and privacy, it will monitors and filters incoming and outgoing network traffic based on predefiend security rules allowing only authorized traffic and blocking malicious or unauthorised access attempts. It will help monitoring network traffic and logging activity, which helps detect suspicious behaviour and support security auditing and compliance. It helps blocking malware, viruses, ransomware and other harmful software before they can infiltrate the network and cause damage. It enforcing access controls so that only trusted user and devices can communicate with the network, which is especially important for remote workers and cloud services. We can restrict and customised communication between on-premise network, internet and servers, it will help to maintain the confidentiality and showcase the importance of security.]

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

[Having different areas in our network for web servers and database servers, offers several significant benefits, It enhanced security, improved traffic management, better network performance.

Security > Placing web server and database server in separate areas (subnets) allows us to isolate resource based on their exposure and function. placeing webserver in public subnet and databade server in privata subnet reduce the attack surface and protects sensitive data by restricting direct access to databases.

Traffic management > Subnets helps in controlling the flow of data in between different types of servers, it's minimize unnecessary broadcasting and congestion across the network.

Having distinct areas allowes network administrators to organised resource logically and making it easier to monitor, troubleshoot, and manage access controls effectively. This can help meet regulatory requirements by separating sensitive worklods from publicly accessible once.]

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

[VPN(Virtual Private Network) provides a secure, encrypted connection between our device and the file storage server, ensuring that all data transferred to and from the server is protected from interception by outsiders. It will encrypts routs through a VPN server and adding a layer of privacy and security. This ensures sensitive files and information remain confidential during upload and download, protecting against hackers, data breaches. It will make our ip address, preventing profiling, enable secure remote access to the file storage server, it will help remote workers accessing internal resources from outside the local network.]

Section 2: Building a secure Network Architecture in VirtualBox

Network Setup

Following the favorable reception of your network diagram, management is keen to see this blueprint come to life in a test environment. They have chosen VMware as the platform to host this venture into the cloud. our next task is to build the test network, which is detailed below.

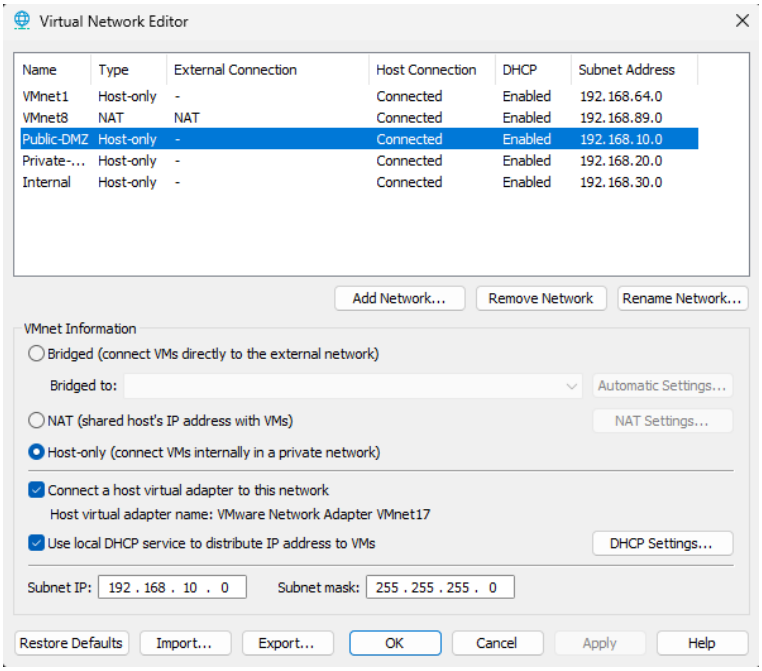
- *Construct two* VMware *virtual networks (VNet):*
  - *Name the first VNet DMZ. Within it, create two subnets:*
    - *Public-DMZ for future web servers.*
    - *Private-DMZ for database servers.*
  - *Name the second VNet Internal and create one subnet within it called Internal-Subnet.*
- *Take and submit a screenshot of the DMZ Virtual Network with the two subnets*
- *Take and submit a screenshot of the Internal Virtual Network with the subnet*

Project Information Slide

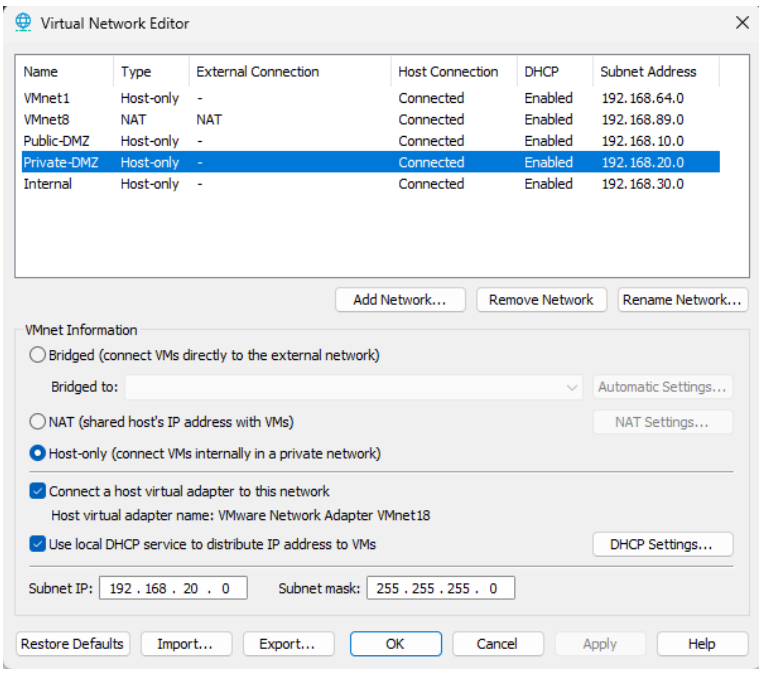
Network Setup of *DMZ Virtual Network*

Note : As we don't have an option to split a particular VNET into two different subnet, create two different adapter with two different subnet for VNET DMZ (using VMware workstation hypervisor).

Public-DMZ



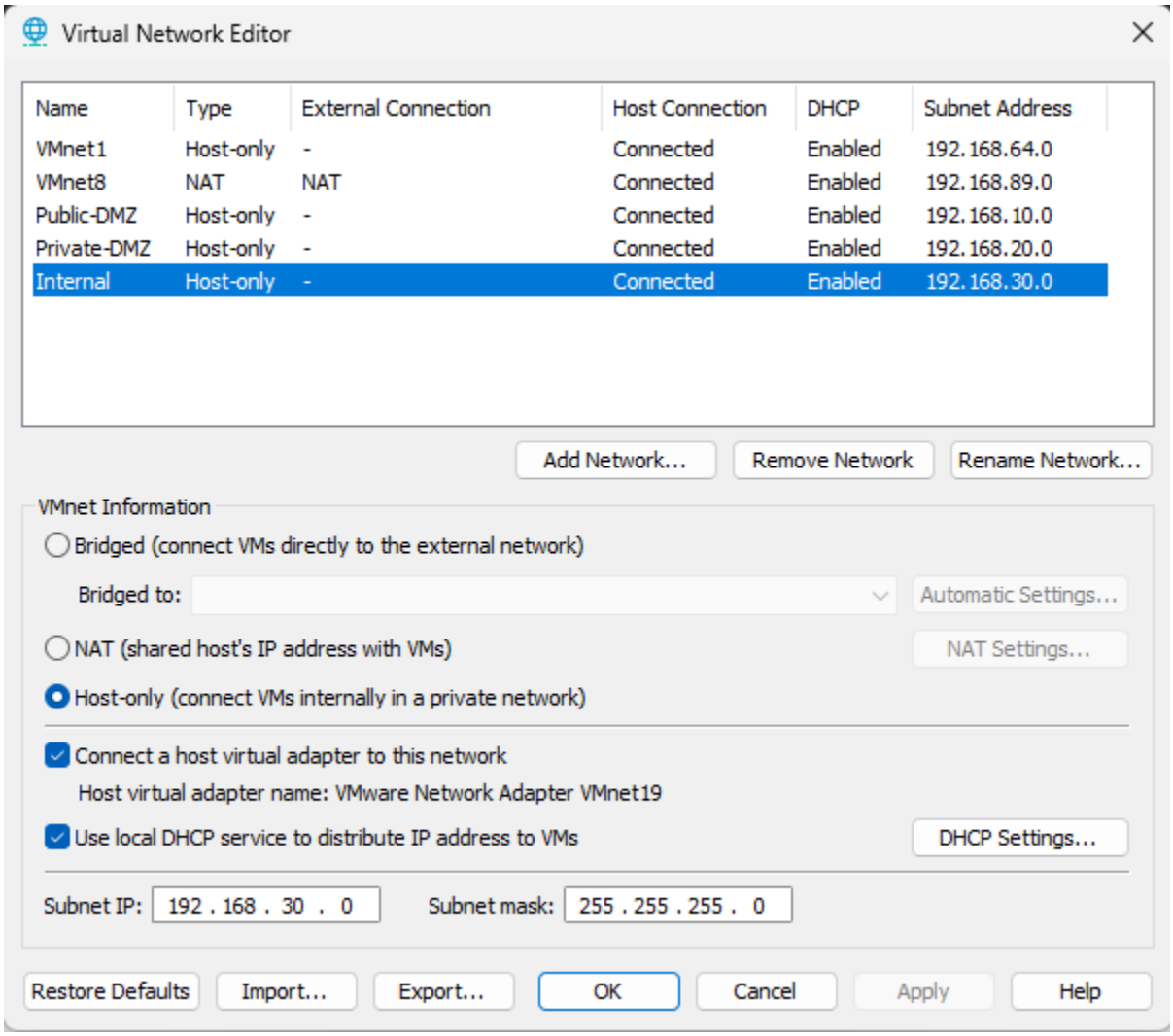
Private-DMZ



Project Information Slide

Network Setup of INTERNAL virtual network

Internal-subnet



Section 3: Continuous Monitoring with a SIEM

Understanding SIEM Benefits

As cyber threats evolve, staying ahead with proactive monitoring is crucial. It's time to get everyone on board with adding a SIEM system to the network. Our task is simple but crucial: convince the stakeholders by pinpointing three major benefits of implementing a SIEM.

- Identify at least 3 distinct benefits of implementing a SIEM in an enterprise environment
- Write a short description of each benefit

Understanding SIEM Benefits

1. [Centralized Security Monitoring]

[SIME helps to gain unified view of security across all IT systems and infrastructure, including cloud and on-premises enviroments. SIEM collects an aggregate data from various sources such as servers, network devices, endpoint and applications. this centralized visibility allows security team to monitor the entire IT environment from a single location helping them to detect potential threat more efficiently. This consolidation aids in better situational awareness and prioritization of threats.]

2. [Reduced incident response time]

[SIME platforms provide real-time alerts and automate response workflows, which help security teams react quickly and effectivly. SIME system analyze incoming event data in real time allowing for the rapid detection of suspicious activities or patterns. by corelating events from different sources a SIEM can identify complex attack scenarios that might go unnoticed when considering individual eversion isolation. This streamlines the containment and mitigation of incidents, minimizing damage and recovery time.]

3. [Forensic Analysis and Incident Investigation]

[In the event of a security breach SIEM's historical data and logs can be used for forensics analysis, this allows security team to trace the origin of the attack identifying the effected systems and understand the attackers tactics thickness and procedure (TTP). SIME tools maintain detailed event logs and correlations required for deep forensic analysis, which is crucial for understanding attack vectors and improving defenses.]

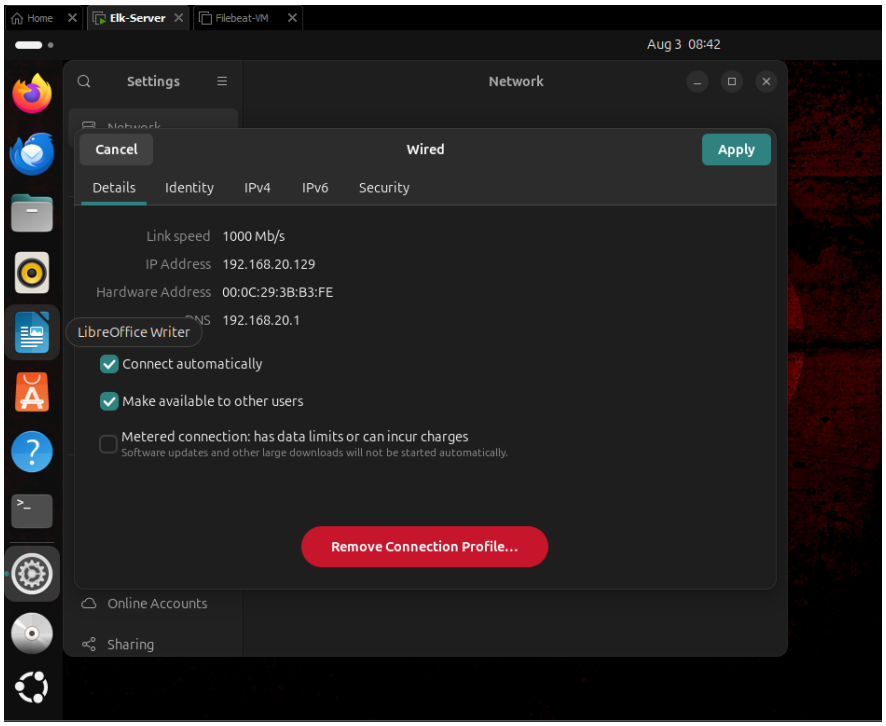
Deploy SIEM Components in VirtualBox

To give management a tangible understanding of how a Security Information and Event Management (SIEM) system operates, we're going to set up a demonstration in our VMware test environment. This setup will involve deploying a virtual machine for the ELK server within the private subnet and a virtual machine for Filebeat within the public subnet. These components will work in tandem to illustrate the power of centralized logging and real-time analysis.

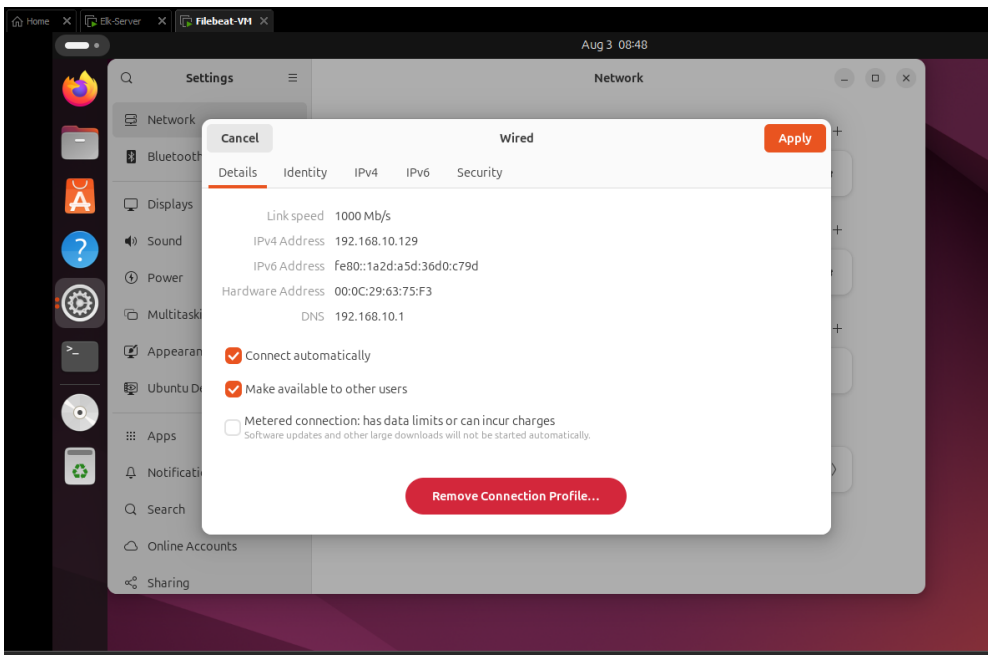
- *Deploy a virtual machine named Elk-Server in the Private-DMZ subnet of the DMZ VNet for the ELK stack.*
- *Deploy a virtual machine named Filebeat-VM in the Public-DMZ subnet of the DMZ VNet for Filebeat.*
- *Take and submit screenshots of the VM instances confirming their creation and network placement.*

Project Information Slide

The VM creation and network placement :
Elk server with private DMZ subnet.

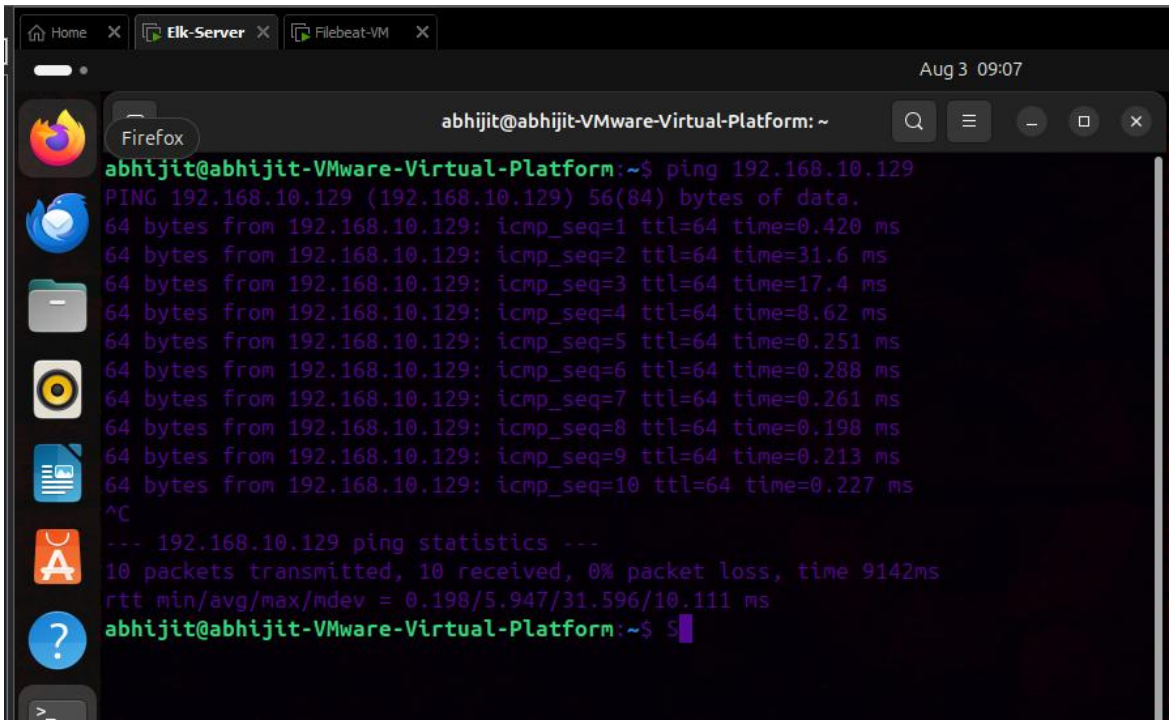


Filebeat-VM with public DMZ subnet.

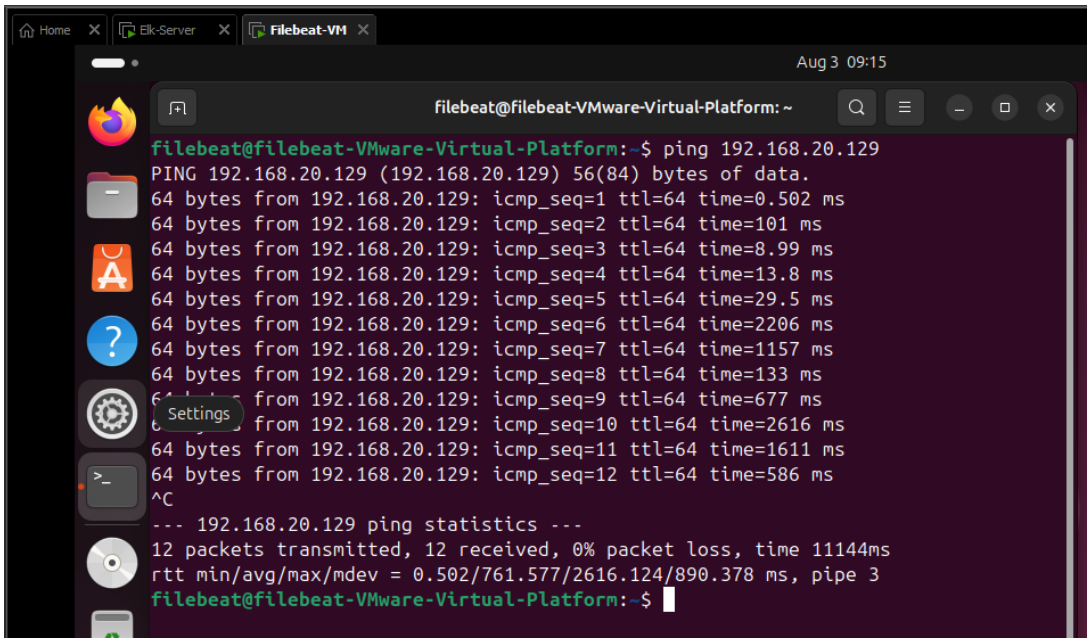


Project Information Slide

Ping from ELK to Filebeat system.



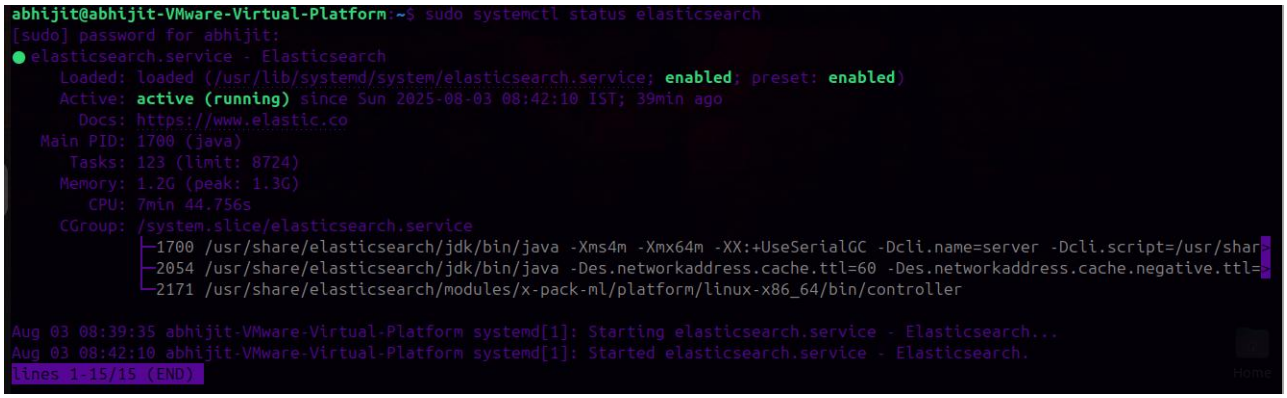
Ping from Filebeat to ELK system.



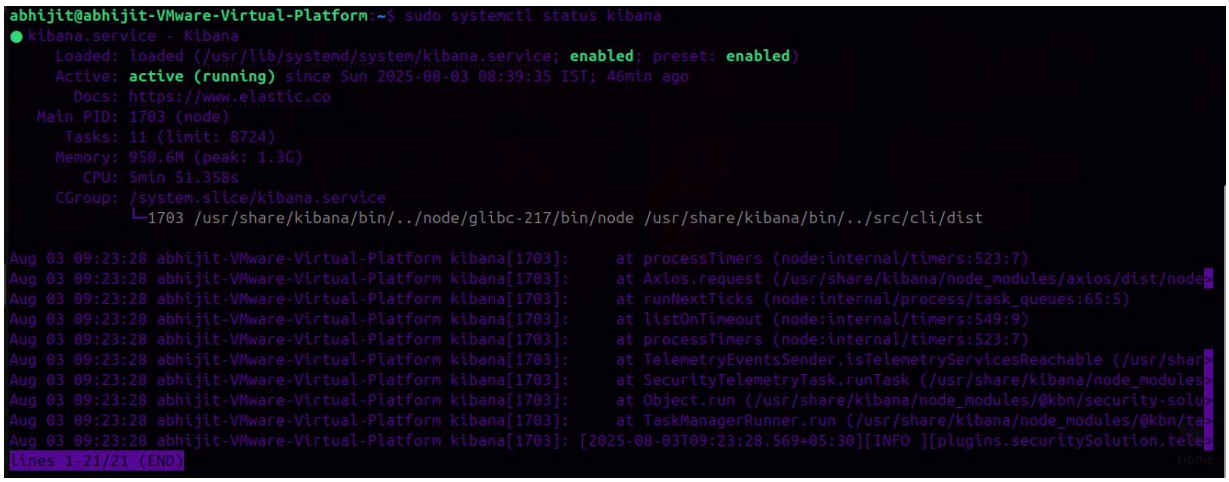
Project Information Slide

Deploy SIEM Components in VMware

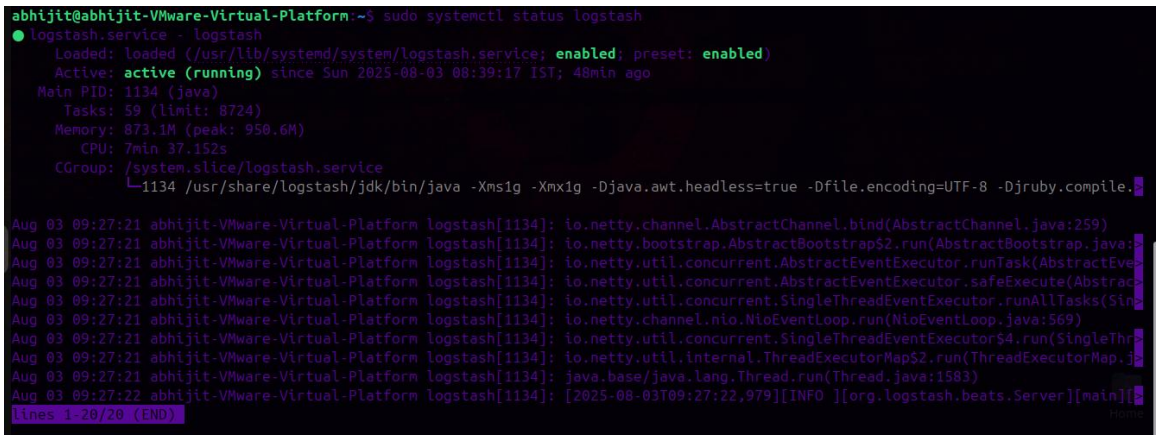
Elasticsearch



Kibana



Logstash



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*

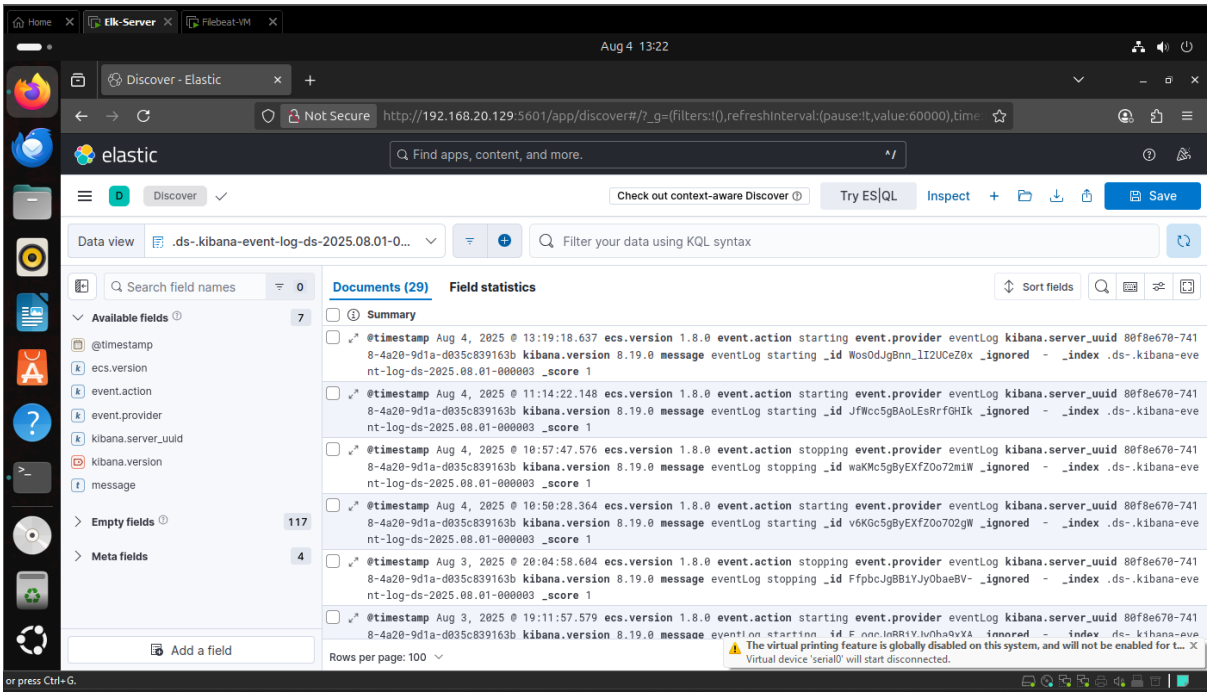
Setup Monitoring

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 4: Zero Trust

Zero Trust Comparison

Following a significant security breach at XYZ, the necessity to reassess and strengthen our network security architecture is paramount. A comparison between the emerging Zero Trust architecture and traditional network security models will highlight the potential enhancements Zero Trust can offer. Our task involves selecting three key principles from Zero Trust architecture, comparing them to traditional models, and evaluating the benefits of Zero Trust. This analysis is crucial for guiding XYZ towards a more resilient cybersecurity framework.

- Select three principles of Zero Trust architecture (We can find them in the classroom and in the next page)
- Compare each selected principle to its counterpart in traditional network security models, focusing on:
  - Differences in approach
  - Potential benefits of Zero Trust over traditional methods

Zero Trust Principles

We will select three principles to use in the comparison:

- Consideration of all resources: Every device, software, and system is a potential security vector.
- Secured communication: Encrypt all data transfers, irrespective of location.
- Per-session access: Grant access to resources only for the duration of a session.
- Dynamic access policy: Access is based on real-time evaluations of multiple factors.
- Continuous monitoring: Real-time assessment of asset integrity and security.
- Dynamic authentication: Ongoing verification before allowing access.
- Extensive data collection: Gather detailed information for security enhancement.

Zero Trust Comparison

1. [Consideration of all resources]	
Zero Trust Approach: [Every device, user, system, and software is seen as a potential security risk and must be continuously verified, regardless of its network location. It's erases the boundary between internal abd external, requring verification for any resource at any time.]	**Traditional Approach:** [Assumes that all resources within the network perimeter are trustworthy by default, focusing on blocking only outside threats and unauthorised access at the boundary, with less security once inside.]
Benefits of Zero Trust:[Zero trust is better equipped for today's fragmented, cloud-based environments by not assuming any internal resource is safe.This mitigates risks free insider threats and unmanaged devices, unlike traditional models that can be blindsided by a breach inside the peramiter.]	

2. [Continuous monitoring]	
Zero Trust Approach: [It will continuously monitor asset integrity, user activity and security status, allowing for real time threat response, enabling rapid detection and response to anomalies. It is proactive and real-time.]	**Traditional Approach:** [Primarily relies on periodic monitoring and auditing, often replying on perimeter devices or logs, with delayed detection and response to incidents. Traditional systems are more reactive and periodic.]
Benefits of Zero Trust:[Zero trust enables proactive threat detection and containment, minimizing damage from breaches. It helps with early detection of breaches and rapid mitigation,reducing overall incident impact.]	

Zero Trust Comparison

3. [Dynamic authentication]	
Zero Trust Approach: [Requires repated and ongoing identity verification like multifactor authentication, device chack for every access attempt. It conducts ongoing verification at every stape, not just at login. It authenticates user dynamically and repeatedly.]	**Traditional Approach:** [Typically authenticates users once, relies mostly on static credentials, such as password, checked primarily at initial login.]
Benefits of Zero Trust:[Attackers cannot exploit old or stolen credentials for extended periods, reducing unauthorized access risks.]	

The Zero Trust Model

Following your analysis of Zero Trust versus traditional security models, it's clear that a Zero Trust framework is essential for enhancing XYZ's network security. The challenge now shifts to selecting the most appropriate Zero Trust model for XYZ from three distinct options: Device Agent & Gateway, Enclave Gateway, or Resource Portal. This selection is critical, as it must align with the unique challenges and goals of the company. Your task is to make an informed choice and articulate why this model stands out as the best fit for XYZ, considering their need for a robust response to recent security vulnerabilities.

- Choose one Zero Trust model for XYZ from the following options:
  - Device Agent & Gateway
  - Enclave Gateway
  - Resource Portal
- Justify why the selected model is the best fit for XYZ's current network challenges and security objectives.

Zero Trust Model

[Device Agent & Gateway]

[justification :

How the model addresses XYZ's specific security challenges?

In this model each enterprise device runs a device agent that brokers access to resources through a gateway. The agent communicates with a policy engine to evaluate and enforce access policies, and sets up a secure, direct, encrypted channel between the device and the resource gateway. The session ends when the task or workflow completes, or security signals occur like timeout or reauth fail. Can enforce security policies right at the device, enabling dynamic, risk-based access control. Offers the ability to terminate connections based on policy changes or detection of threats.

Why it aligns with XYZ's security objectives and current network situation?

Company like XYZ especially those with a mix of hybrid work, a managed device fleet, and moderate IT complexity – the Device Agent & Gateway Model is recommended as the primary zero trust architecture. It provides the highest level of fine-grained policy enforcement, device security, and continus monitoring, also supports dynamic, risk-based access and protection against insider and sophisticated external thereats. Based on the current network sitution it offers the highest level of securitu and flexibility, session-based control and continuous device health validation. As XYZ manages its endpoints well, this approch will enable the strongest Zero trust posture becomes more distributed and cloud-connected.]