SECURING THE PERIMETER

[Samala Raghavaraj]
[CBS-0327]

Project Scenario

Project Information Slide

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.

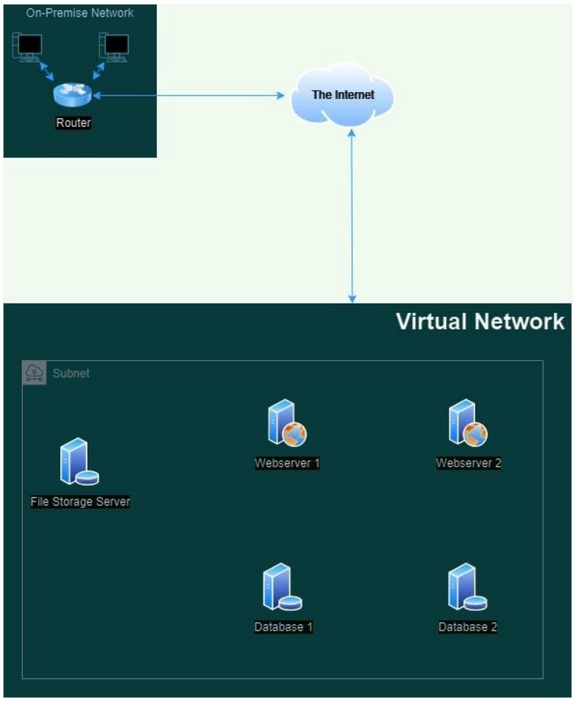
Due to a lack of visibility and a lack of proper access control setup on the network, it was inevitable that a breach took place! XYZ was hit with a massive attack in which their network was breached and their internal servers were compromised resulting in over 500 Bitcoin being stolen!

To address these vulnerabilities, XYZ has engaged SecureCorp, a global cybersecurity consulting firm, to redesign its network architecture and implement a Security Information and Event Management (SIEM) system to provide continuous monitoring and protection against future attacks.

Project Information Slide

Network Description

Download the [drawio.com]() file [from here.]()



- *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.*

Section 1:

Designing a secure Network Architecture

Network Vulnerabilities

1. No Network monitoring (SIEM/IPS/IDS)

Issue : There Is no network monitoring , Detection and prevention Tools from Malicious Attacks or Threats

Risk : 1) Suspicious Activity or Attacks (like Brute force , Port Scanning , Malware Threats) are go undetected

2) There is no Visibility into Who is accessing and Suspicious activity in Network

3) Without Monitoring threats can remain Undetected go for long time and escalate their Access or Steal data or Misconfigured the Data or Transfer Funds

4) Direct exposure Of Resources to the internet can increase the chance of attacks and Threats

Fix : deploy tools like SIEM to collect logs and detect anomalies in real time and Create a Firewalls (Set some predefined rules) , Implement IDS/IPS

2) SIEM Is a centralized Monitoring and It process logs and dashboard to view

2. No Network Segmentation

Issue : All servers (web servers , Databases and File server) are all in the Single Subnet with Virtual Network

Risk : 1) If One server is attacked easily attacker gain or compromise the other resources also because all are in a single subnet

2) By gaining the resources they can steal the data or Do suspicious Activity in network It leads to massive threats which compromise all the Network Down

Fix : By Segmenting the Servers as Public Subnet for Web servers and Private Subnet for File storage and databases And Lastly Applying the Firewalls and MFA For to Access the Data

Project Information Slide

Network Vulnerabilities

3 . No Data Protection and Backup server

Issue : In The Network Architecture There is no Data backup Server and And Data Protection plan
Risk : 1) There are two databases in the architecture if the Admin or Developer if he accidently deleted the data its not recoverable
2) If the attackers Attack the Database Servers and file servers they can demand ransomware
3) If there is a system failure or Any Hardware related or any problem in server it can cause the data lost
4) We risk our Total data Loss with No recovery Option
5) Non compliance with Data regulation (GDPR,ISO) backup plans are missing
Solution :1) By adding a backup server to store the data
 2) Use automated Backups for databases and file servers

Project Information Slide

Network Redesign

https://drive.google.com/file/d/1bHz8-waUewozUpuu2muvQyu0szsNdxig/view?usp=sharing

- This diagram illustrates a **secure network architecture** that integrates multiple security controls across **on-premise, public subnet, and private subnet** environments.

Project Information Slide

Convincing the Stakeholders

Why do we need to add firewalls to our network?

A Firewall is a security System that Constantly Monitors and Filters Both Incoming and outgoing traffic depending upon the predefined Security policies

Pros :

1) Traffic filtering : The firewall allows only the traffic that based on predefined rules Like(Block all traffic except HTTPS)
2) Intrusion prevention : firewalls blocks malicious access attempts from hackers and malware
3) We can allow trusted ips only
4) Helps meet Compliance standards (GDPR, ISO 27001)
5) Fire walls reduce the risk of Security breaches and service disruptions

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

We segmented the area of Web server as public subnet and the Database servers and file servers as private subnet

1) we divided the Sensitive data and files with segmenting the network

2) In future if attackers Attack the web servers , we can easily isolate and due to segmentation our database servers are secure (attackers cannot access the databases

3) better performance and security per layer , We can easily Monitor and detect any suspicious activity

4) malware or viruses cannot move across networks

5) Increases resilience one compromised system wont bring down the entire Network Expose

Convincing the Stakeholders

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

A VPN (Virtual private network) Its create a secure encrypted connection between the on-premise network and the cloud or external network

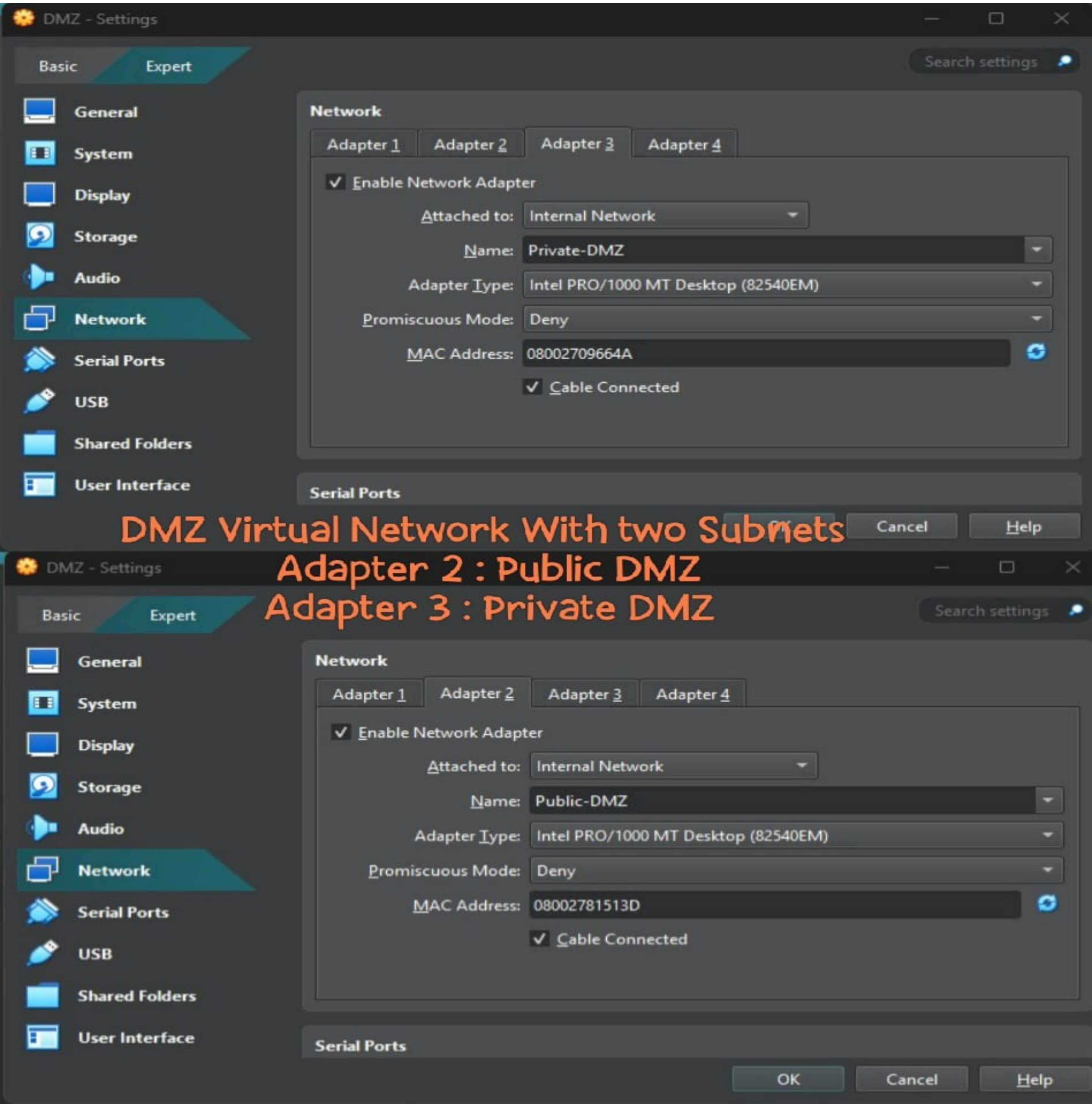
1) When we use data or do transist data – it encrypts the data and Also Stops the MITM attacks
2) It ensures only authorized Internal USers can Access the data or file server
3) It helps us to prevent exposure to the public internet
4) Authentication : VPNs Require credentials or certificates to connect – ensuring only authorized users can access
5) Adds a security layer for external access

Protects Intellectual property and internal files from external threats while enabling remote or hybrid work securely

Section 2:

Building a secure Network Architecture in VirtualBox

Creating DMZ and Internal Network Architecture in VirtualBox



DMZ Virtual Network With two Subnets
Adapter 2 : Public DMZ
Adapter 3 : Private DMZ

DMZ - Settings

Network

Adapter 3

☑ Enable Network Adapter

Attached to: Internal Network

Name: Private-DMZ

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 08002709664A

☑ Cable Connected

DMZ - Settings

Network

Adapter 2

☑ Enable Network Adapter

Attached to: Internal Network

Name: Public-DMZ

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

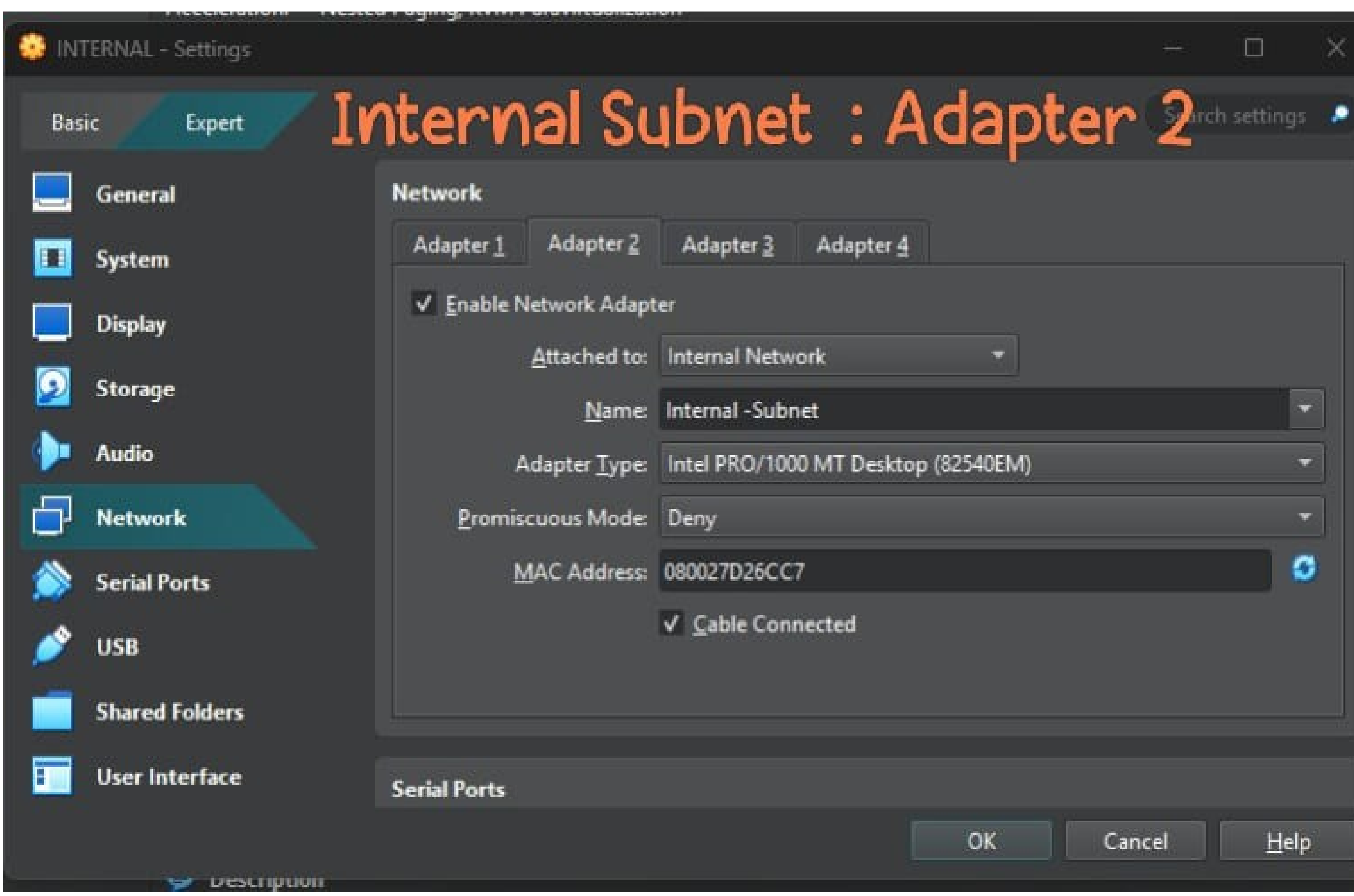
Promiscuous Mode: Deny

MAC Address: 08002781513D

☑ Cable Connected

Project Information Slide

Creating DMZ and Internal Network Architecture in VirtualBox



Internal Subnet : Adapter 2

INTERNAL - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: Internal Network

Name: Internal -Subnet

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027D26CC7

☑ Cable Connected

Section 3:

Continuous Monitoring with a SIEM

Project Information Slide

Understanding SIEM Benefits

1. Real time threat detection and monitoring

SIEM collects and analyzes logs from across the network in real time to identify suspicious behaviour or known attacks acc to patterns

- Immediate alerts for Suspicious behaviour or malicious or unusual traffic
- It easily detects the Threats before breaches happen
- We can set predefined rules for endpoints or some behaviour patterns
- Even it blocks the suspicious activity in network or system behaviour and it generates the alerts to IT Team
- Reduce risk of data loss and attacks or any loss by Monitoring and detecting

2. Centralized View Of Entire Network

One Of the best of SIEM Is Centralized view of Entire network , It's A central platform that collects , analyzes and Correlates security logs from network

- Single dashboard to view logs from all devices (Servers, endpoints, firewalls,Network, applications,cloud platforms)
- Helps in faster incident investigation and response if any threat happen
- Reduces the threats and simplifies troubleshooting
- Helps to see events and reduce the workload and provides clarity during a any problem

Project Information Slide

Understanding SIEM Benefits

3. Regulatory Compliance

Automatically logs , stores and reports security events – with built in tools for compliance Standards LIKE GDPR , HIPPA, PCI-DSS , ISO 27001

* By viewing of logs and events Makes audit faster and easier

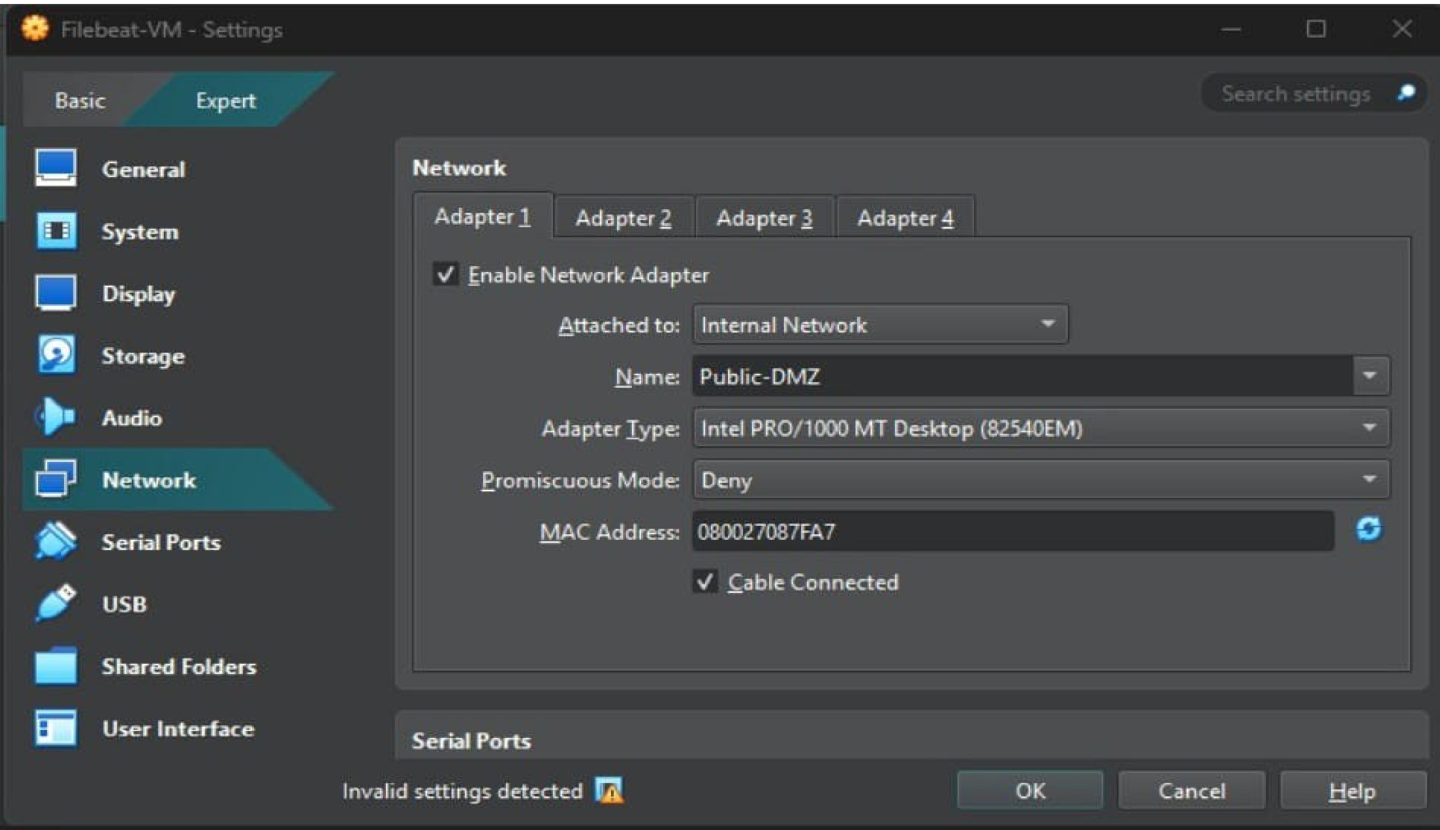
- Ensure the Legal requirements
- Generates Audit ready reports and stores logs securely
- Avoids fines or regulatory penalties and reputational damage
- Helps also Maintain trust among the Clients and users and position as a secure and compliant organization

Deploy SIEM Components in VirtualBox

A VirtualBox-based test environment was configured to demonstrate the operation of a Security Information and Event Management (SIEM) system.

A virtual machine named **Elk-Server** was deployed in the **Private-DMZ** subnet of the DMZ VNet to host the ELK stack (Elasticsearch, Logstash, Kibana). Another virtual machine named **Filebeat-VM** was deployed in the **Public-DMZ** subnet of the DMZ VNet to run Filebeat, which collects logs and forwards them to the ELK server.

Project Information Slide



Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: Public-DMZ

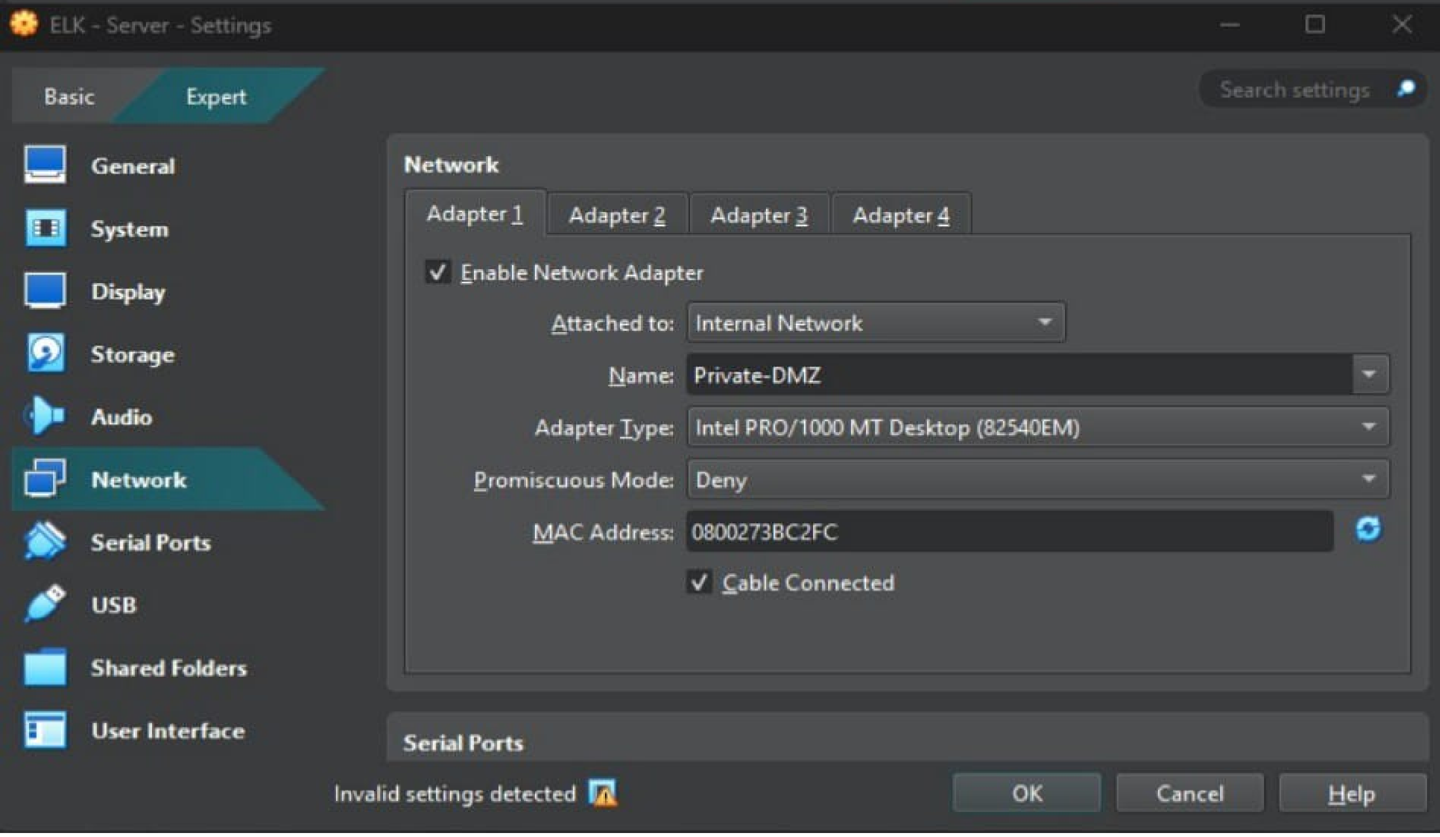
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027087FA7

☑ Cable Connected

Invalid settings detected



Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: Private-DMZ

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 0800273BC2FC

☑ Cable Connected

Invalid settings detected

Project Information Slide

Setup Monitoring

To showcase the capabilities of the SIEM system, an ELK (Elasticsearch, Logstash, Kibana) server was set up within the **Private-DMZ** subnet, and Filebeat was installed on a web server located in the **Public-DMZ** subnet.

Filebeat was configured to forward web server logs to the ELK server's Elasticsearch service. Log data was generated by accessing the web server, allowing real-time monitoring of activity through Kibana.

Verification was performed to ensure:

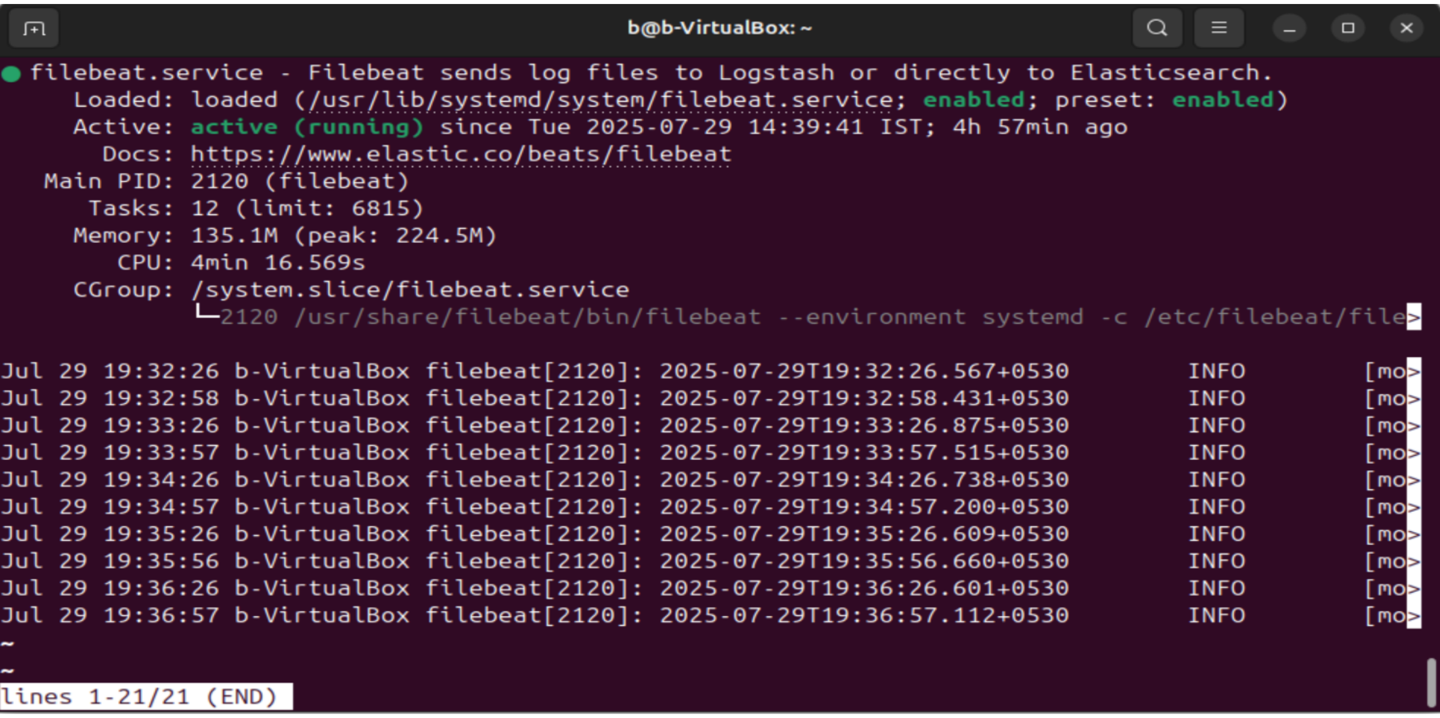
- The **Filebeat service** was actively running on the web server.

- **Kibana** successfully received and displayed logs from the Filebeat host in the *SIEM* → *Hosts* → *Filebeat-VM* section.

Project Information Slide

Setup Monitoring

Filebeat service status on the web server, confirming that the service is active and running.

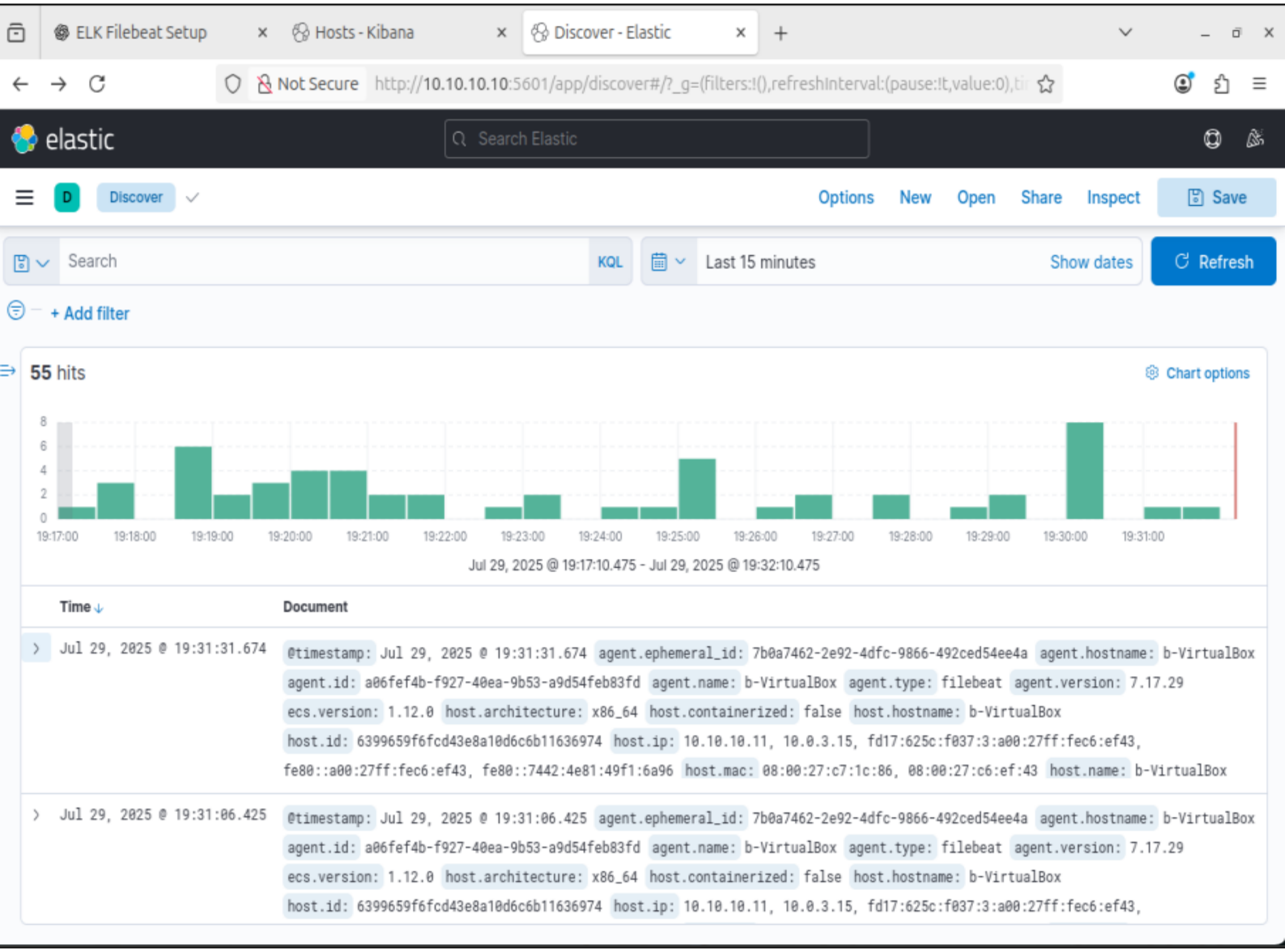


```
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
     Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-07-29 14:39:41 IST; 4h 57min ago
       Docs: https://www.elastic.co/beats/filebeat
   Main PID: 2120 (filebeat)
      Tasks: 12 (limit: 6815)
     Memory: 135.1M (peak: 224.5M)
        CPU: 4min 16.569s
     CGroup: /system.slice/filebeat.service
             └─2120 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/file>

Jul 29 19:32:26 b-VirtualBox filebeat[2120]: 2025-07-29T19:32:26.567+0530        INFO        [mo>
Jul 29 19:32:58 b-VirtualBox filebeat[2120]: 2025-07-29T19:32:58.431+0530        INFO        [mo>
Jul 29 19:33:26 b-VirtualBox filebeat[2120]: 2025-07-29T19:33:26.875+0530        INFO        [mo>
Jul 29 19:33:57 b-VirtualBox filebeat[2120]: 2025-07-29T19:33:57.515+0530        INFO        [mo>
Jul 29 19:34:26 b-VirtualBox filebeat[2120]: 2025-07-29T19:34:26.738+0530        INFO        [mo>
Jul 29 19:34:57 b-VirtualBox filebeat[2120]: 2025-07-29T19:34:57.200+0530        INFO        [mo>
Jul 29 19:35:26 b-VirtualBox filebeat[2120]: 2025-07-29T19:35:26.609+0530        INFO        [mo>
Jul 29 19:35:56 b-VirtualBox filebeat[2120]: 2025-07-29T19:35:56.660+0530        INFO        [mo>
Jul 29 19:36:26 b-VirtualBox filebeat[2120]: 2025-07-29T19:36:26.601+0530        INFO        [mo>
Jul 29 19:36:57 b-VirtualBox filebeat[2120]: 2025-07-29T19:36:57.112+0530        INFO        [mo>
~
~
lines 1-21/21 (END)
```

Project Information Slide

Kibana interface confirming receipt of logs from the Filebeat host (SIEM → Hosts → Filebeat-VM).



```
Jul 29, 2025 @ 19:31:31.674   @timestamp: Jul 29, 2025 @ 19:31:31.674 agent.ephemeral_id: 7b0a7462-2e92-4dfc-9866-492ced54ee4a agent.hostname: b-VirtualBox
                              agent.id: a06fef4b-f927-40ea-9b53-a9d54feb83fd agent.name: b-VirtualBox agent.type: filebeat agent.version: 7.17.29
                              ecs.version: 1.12.0 host.architecture: x86_64 host.containerized: false host.hostname: b-VirtualBox
                              host.id: 6399659f6fcd43e8a10d6c6b11636974 host.ip: 10.10.10.11, 10.0.3.15, fd17:625c:f037:3:a00:27ff:fec6:ef43,
                              fe80::a00:27ff:fec6:ef43, fe80::7442:4e81:49f1:6a96 host.mac: 08:00:27:c7:1c:86, 08:00:27:c6:ef:43 host.name: b-VirtualBox

Jul 29, 2025 @ 19:31:06.425   @timestamp: Jul 29, 2025 @ 19:31:06.425 agent.ephemeral_id: 7b0a7462-2e92-4dfc-9866-492ced54ee4a agent.hostname: b-VirtualBox
                              agent.id: a06fef4b-f927-40ea-9b53-a9d54feb83fd agent.name: b-VirtualBox agent.type: filebeat agent.version: 7.17.29
                              ecs.version: 1.12.0 host.architecture: x86_64 host.containerized: false host.hostname: b-VirtualBox
                              host.id: 6399659f6fcd43e8a10d6c6b11636974 host.ip: 10.10.10.11, 10.0.3.15, fd17:625c:f037:3:a00:27ff:fec6:ef43,
```

Section 4:

Zero Trust

Project Information Slide

Zero Trust

Given XYZ's recent security incidents and the weaknesses identified in its current perimeter-based security model, implementing Zero Trust principles is a strategic necessity. The following slide summarizes the key benefits and justifications for adopting the Device Agent & Gateway Zero Trust model, based on the detailed analysis of Dynamic Access Policy, Per-Session Access, and Continuous Monitoring principles.

Zero Trust Comparison

1. Dynamic Access Policy

Zero Trust Approach: Access decisions are made dynamically based on real time analysis of user behavior,device health ,location and risk level , even if we are from internal network we doesnt get automatic access just because were inside the company , it checks who we are and all

Temporary , least-privilege access: Zero trust

Traditional Approach: the traditional approach is like if we once login in a website or any account until we logged out or for a long time or sometimes all day until someone remove manually removes access or we exit or logout

Mostly it's based on your roles

Traditional : long-lasting access once authenticated

Benefits of Zero Trust : The Zero trust when it logins it limits the exposure window if credentials are compromised

It only give access when everythings looks safe or it will block

It reduces the chance of attacks , which it checks all or it verifies first and allows it , whether internal or external

Responds automatically to changing threat levels or anomalies

2. Per-Session access

Zero Trust Approach: The access needs to the system is for a short time , When the session ends the access also ends too

Access is granted only for the specific session and scope required , Each new session requires fresh authorization

Its like a giving someone a one-time pass that expires quickly

Traditional Approach: If a users stay logged in for hours or even days , and they might retain access to systems even they don’t always need

If someone logs in to the Internal network they can often use multiple access without being asked again

Benefits of Zero Trust: It reduces the time window for attacks : if someone session is hijacked , it won't last long

Principle of least privilege access : the access will get based on the basis of user role what tehy need and only for as long as they need it and then it expires or re authentication

If an attacker manages to get in , their access will be temporary and limited making it harder to cause damage

Zero Trust Comparison

<table>
<tr><th colspan="2">3. Continuous Monitoring</th></tr>
<tr><td><b>Zero Trust Approach:</b> IN zero trust Systems and Endpoints , Applications are always Monitoring Activities in real time
 * It looks always for strange or risky behaviour in real time and reacts quickly it blocks or keep in Isolation and also alerts to the IT Team
* Continuously monitors all security postures in real time to detect any Suspicious
* It Looks for Strange patterns in network or system continuously monitors</td><td><b>Traditional Approach :</b> The traditional security looks for something gone wrong then checks the logs or alerts after the attack has already happened
* Monioring is often passive or delayed , logs may be collected but only reviewed if a problem is noticed
* it reviews the audits and logs after an incident</td></tr>
<tr><td colspan="2"><b>Benefits of Zero Trust:</b> : If we see the zero trust IT finds the problem early , before damage happens , IF anything happen suspicious it automatically block suspicious activity
Real time monitoring stops threats as they happen and Tighter control , less damage when something goes wrong , It helps the company stay one step ahead of attackers
Faster threat detection and response passive and real time analysis</td></tr>
</table>

Project Information Slide

Zero Trust Model

Device agent and Gateway
Acc to our XYZ Scenario has been a security problems uncontrolled lateral movement and weak identity verification and less device security - In this Context the device Agent and Gateway model offers the most comprehensive and enforceable zero trust approach and strong access control , visibility and trust * Device requires a agent to authenticate and continuously assess trust before it connects , It ensures up to date endpoints are allowed to access internal services * The gateway enforces policies per session , isolating network access to only what the user/device needs - Mitigation of lateral movement * Device agents can monitor traffic , log user actions and provide visibility to the security team and supports incident response and forensics and recovering from abreach * Agents and gateways ensure strict environment and the gateway can block access for compromised devices in real time * Continuous logging and trust verification support regulatory needs