SECURING THE PERIMETER

[NILOTPAL SARMA]
[CBS-0180]

Project Information Slide

HOW TO USE THIS TEMPLATE

- We have provided these slides as a guide to ensure you submit all the required components to complete your project successfully.
- When presenting your project, remember that these slides are merely a guide. We strongly encourage you to embrace your creative freedom and make changes that reflect your unique vision as long as the required information is present.
- You can add slides to the template when your answers or screenshots do not fit on the previously provided pages.
- Delete this and all other project instruction slides before submitting your project.
- **Remember to add your name and the date to the cover page.**

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!

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.

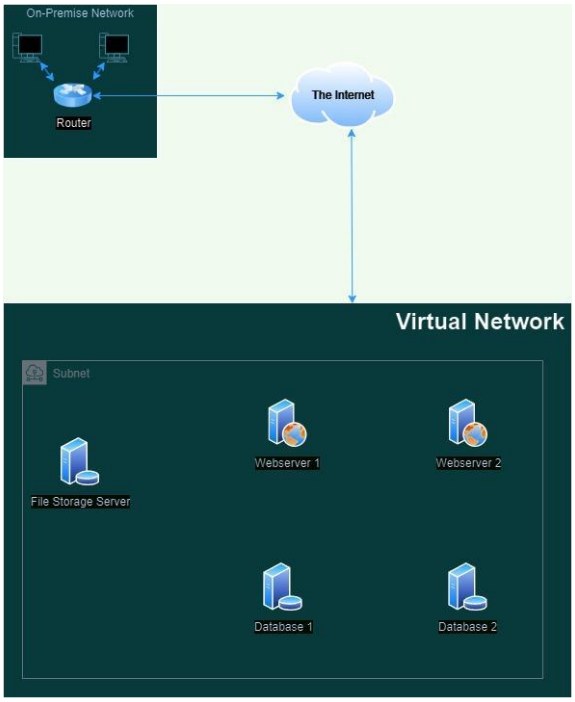
Section 1:

Designing a secure Network Architecture

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.*

Project Information Slide

Identify Network Vulnerabilities

In your initial assessment of the company's network, it's essential to pinpoint specific vulnerabilities that could be exploited by malicious actors. Identifying these weaknesses is the first step in reinforcing the network's defenses.

- *Review the provided network diagram*
- *Identify three major security problems with the current network setup*
- *Describe each identified problem and explain how it poses a risk to the network*

Project Information Slide

Identify Network Vulnerabilities

1. All Servers Have Direct Internet Access

Problem: All five servers (web servers, database servers, and file storage server) have direct access to the internet.

Risk:
- Direct internet access leaves all servers vulnerable to attacks from outside malicious parties.
- Web servers, database servers, and file storage servers are very important parts of the network, and connecting them directly to the internet raises the possibility of unauthorized access, data breach, and SQL injection, DDoS, or Ransomware attacks.
- Data stored on database servers or the file storage server, It can be breached if an attacker gets access to it

2. Simple Network Architecture

Problem: All the five servers are inside the same virtual network and in the same subnet.

Risk:
- Simple network architecture indicates no segmentation between various categories of servers (e.g., web servers, database servers, file storage server).
- Since a single server can be easily pivoted to other servers in the same subnet, compromising the entire network.
- There is no confinement of possible threats, so it is simpler for malware or unauthorized access to propagate throughout the network.

3. Lack of Access Control for the File Storage Server

Problem: The file storage server is accessible from the on-premise network because the On-premise network are connected the Virtual machine via internet directly there is no Firewall on between them and If On-premise network is exploitable by an attacker then It is also exposed to the virtual network.
Risk:
- Without access controls, any device or user on the on-premise network can potentially access the file storage server, resulting in unauthorized access to sensitive information.
- If an attacker compromises the on-premise network, they can easily attack the file storage server and exfiltrate or destroy data.

Project Information Slide

Network Redesign

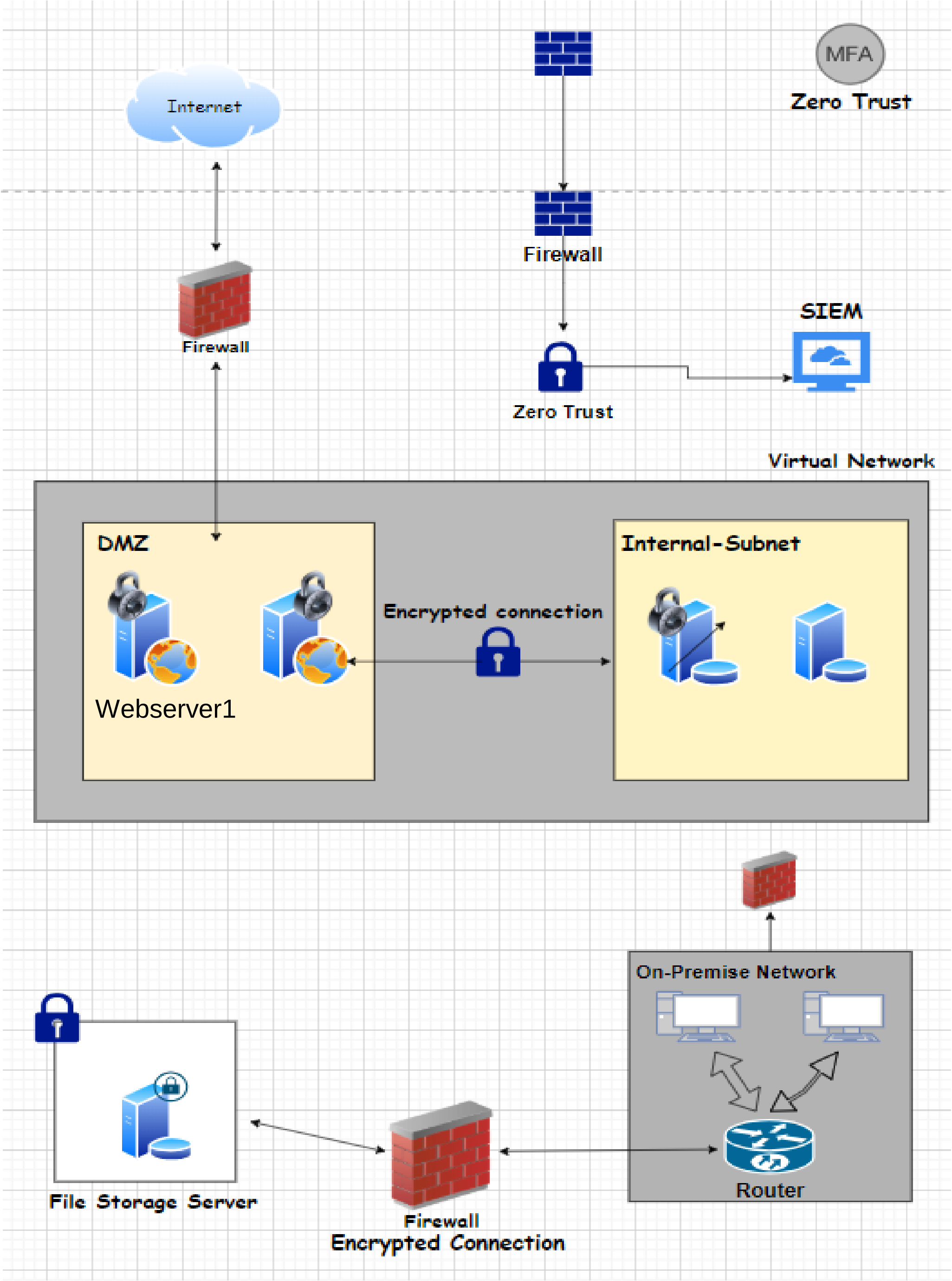
With the vulnerabilities identified, it’s time to rearchitect the network. A well-structured network with proper security controls is vital for defending the company's digital assets.

- 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.*

Project Information Slide

Network Redesign

Place the updated network diagram here.



Project Information Slide

Convince the Stakeholders

With a proposed network redesign, stakeholders will require a clear understanding of the benefits and necessity of these changes. Your next task is to prepare answers to the following potential questions they may have. In all your answers, 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 are important in network security since they provide a barrier which filters and manages network traffic for defense against unauthorized access and malicious attempts, allowing only authorized traffic to enter or leave the network. We need Add Firewall Because of Firewall Provide a Protection against external threats , Firewalls serve as a frontline defense against hackers, malware, and other online threats trying to access your network from the outside .

Management of network traffic:

Firewalls enable you to establish and apply security policies, controlling the traffic permitted or denied based on a range of criteria such as IP addresses, ports, and protocols .

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

Separating web and database servers into different network areas enhances security by limiting potential damage from web server compromises, improving performance by isolating resource-intensive tasks, and enabling better scalability and management

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

VPN is Virtual private network . Bypassing Restrictions If the server containing the file storage is placed in a different region or country that has restricted access to it, then a VPN would aid in bypassing these geographical restrictions by linking your connection from an allowed location. Protection on Public Networks: While connecting to a file storage server over a public Wi-Fi, a VPN conceals the user's data which is in immediate danger of being attacked. As for Data Integrity: A VPN safeguards the data against any form of alteration throughout its transmission by encrypting it which helps in safeguarding the data's information.

Section 2:

Building a secure Network Architecture in VirtualBox

Project Information Slide

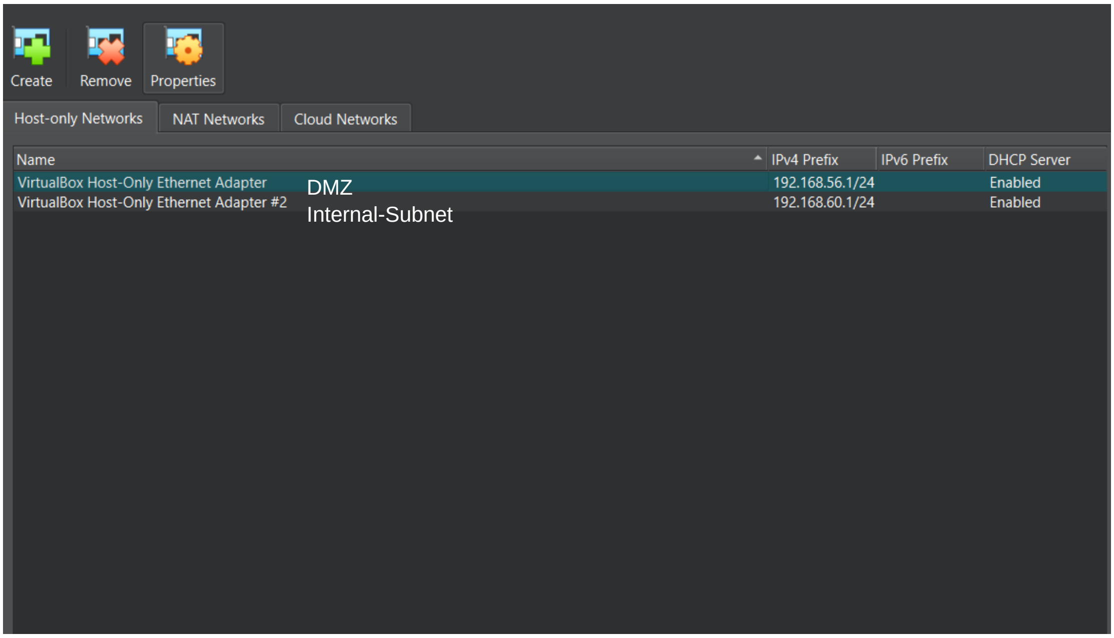
Network Setup

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 VirtualBox as the platform to host this venture into the cloud. Your next task is to build the test network, which is detailed below.

- *Construct two VirtualBox 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*

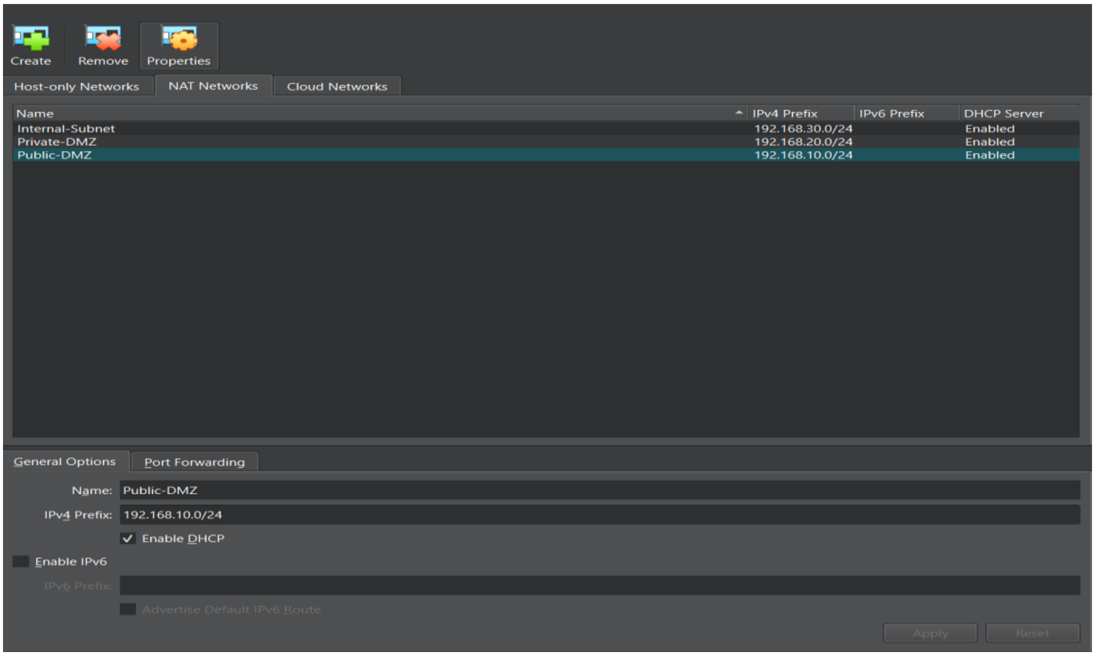
Network Setup

Screenshot of the DMZ Virtual Network with the two subnets



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.168.56.1/24		Enabled
VirtualBox Host-Only Ethernet Adapter #2	192.168.60.1/24		Enabled

DMZ
Internal-Subnet



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
Internal-Subnet	192.168.30.0/24		Enabled
Private-DMZ	192.168.20.0/24		Enabled
Public-DMZ	192.168.10.0/24		Enabled

Name: Public-DMZ
IPv4 Prefix: 192.168.10.0/24
☑ Enable DHCP
□ Enable IPv6
IPv6 Prefix:
□ Advertise Default IPv6 Route

Section 3:

Continuous Monitoring with a SIEM

Project Information Slide

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. Your 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 Production Log Management

The SIEM solution serves as a centralized platform that receives, stores, normalizes, and correlates log data coming from very diverse sources across an organization, thus ensuring no duplication of events. This centralized approach makes log management easier to find, analyze, and correlate from different systems. Centralized log management assures that crucial log data is safely kept and easily retrievable for matters of compliance, incident investigation, and performance analysis.

2. Real-time threat detection and alerts

SIEM solutions continuously monitor the IT environment of any organization in real time and also analyze data logs from sources. Using event correlation facilitated through devices and advanced analytics, it detects complex attack patterns—the ones that would never be sooner carefully noticed by its tools for safety. Such ability to detect threats in real-time enables a security team to react swiftly to potential incidents, thereby minimizing the likelihood of the success of an attack, along with the consequences that it brings

3. Enhanced Visibility and Situational Awareness

SIEM can provide a holistic perspective regarding an organization’s security posture, as it pools and correlates extremely large data sets from various sources in the IT infrastructure. Through this holistic perspective, a security team can pair a general feel for the big picture around security events with patterns outside of visibility that might not raise a flag when drilling down through system after system. Better visibility has resulted in sound situational awareness and allows organizations to make more informed, data-driven decisions regarding good use of security strategy and resource grantees.

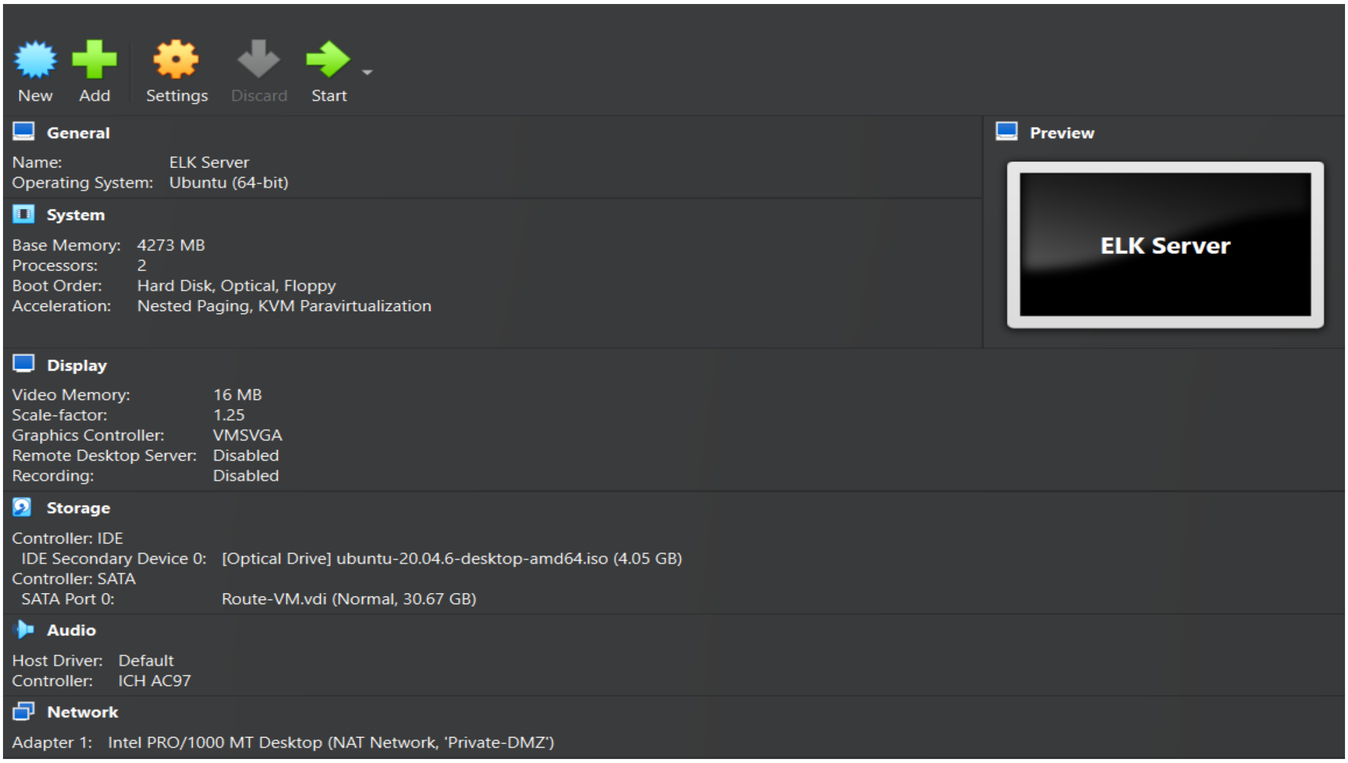
Project Information Slide

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 VirtualBox 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.*

Deploy SIEM Components in VirtualBox



General

Name: ELK Server
Operating System: Ubuntu (64-bit)

System

Base Memory: 4273 MB
Processors: 2
Boot Order: Hard Disk, Optical, Floppy
Acceleration: Nested Paging, KVM Paravirtualization

Preview

ELK Server

Display

Video Memory: 16 MB
Scale-factor: 1.25
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

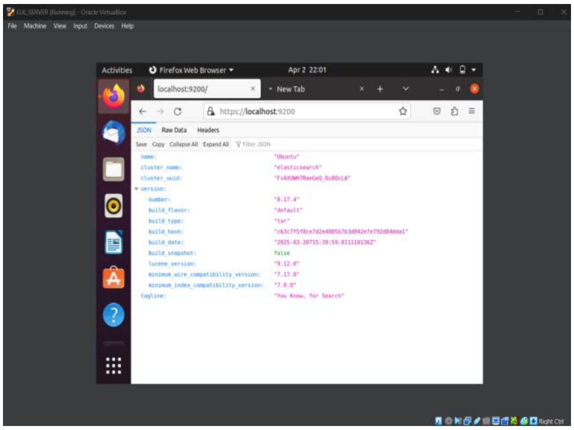
Controller: IDE
IDE Secondary Device 0: [Optical Drive] ubuntu-20.04.6-desktop-amd64.iso (4.05 GB)
Controller: SATA
SATA Port 0: Route-VM.vdi (Normal, 30.67 GB)

Audio

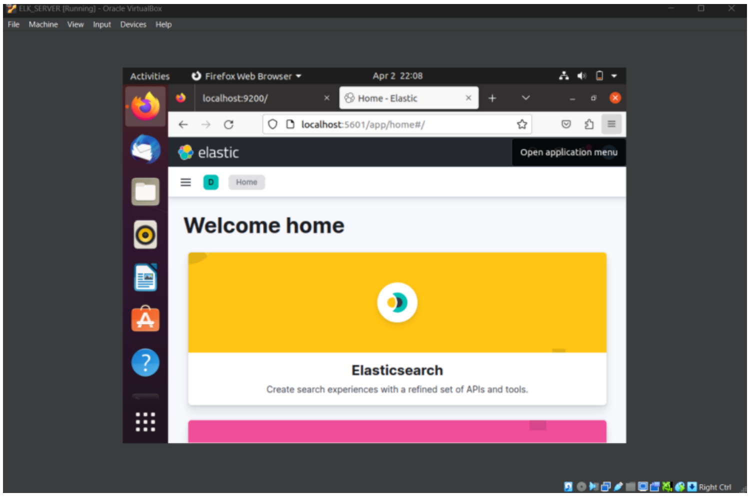
Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'Private-DMZ')



```
name:                                   "Ubuntu"
cluster_name:                           "elasticsearch"
cluster_uuid:                           "FvAXUWH7RaeGeD_Du8QcLA"
▾ version:
   number:                              "8.17.4"
   build_flavor:                        "default"
   build_type:                          "tar"
   build_hash:                          "c63c7f5f8ce7d2e4805b7b3d842e7e792d84dda1"
   build_date:                          "2025-03-20T15:39:59.811110136Z"
   build_snapshot:                      false
   lucene_version:                      "9.12.0"
   minimum_wire_compatibility_version:  "7.17.0"
   minimum_index_compatibility_version: "7.0.0"
tagline:                                "You Know, for Search"
```

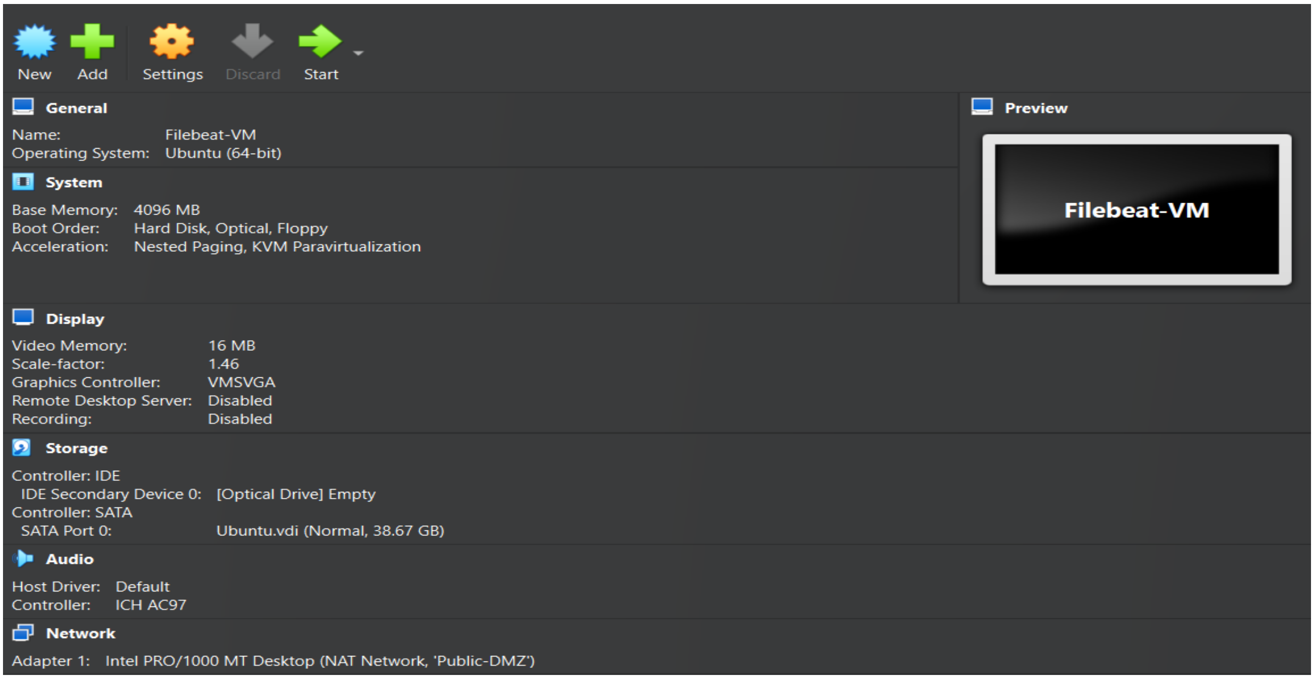


Welcome home

Elasticsearch

Create search experiences with a refined set of APIs and tools.

Project Information Slide



General

Name: Filebeat-VM
Operating System: Ubuntu (64-bit)

System

Base Memory: 4096 MB
Boot Order: Hard Disk, Optical, Floppy
Acceleration: Nested Paging, KVM Paravirtualization

Preview

Filebeat-VM

Display

Video Memory: 16 MB
Scale-factor: 1.46
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Ubuntu.vdi (Normal, 38.67 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'Public-DMZ')

Project Information Slide

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*

Project Information Slide

Setup Monitoring

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

.

[Add Screenshot here]

Project Information Slide

Setup Monitoring

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

[Add Screenshot here]

Section 4:

Zero Trust

Project Information Slide

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. Your 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 (you 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

Project Information Slide

Zero Trust Principles

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.

Project Information Slide

Zero Trust Comparison

1. All resources provide maximum consideration

A Zero Trust model assumes that every device, software, and system could be a possible security threat. This means that both internal and external network resources are considered untouchable by default. Every access request is verified and authenticated with depth

Older security systems tend to have a resource-based security model with a perimeter approach in which network users retrieve resources almost effortlessly. If a resourceful attacker breaches the network, this can be extremely dangerous.

Improved security by greater scrutiny and continuous verification of all resources that mitigate potential threats. In simpler terms, there is enhanced threat detection and response strategies

2. Protected communication

The Zero Trust model brings a unique way of dealing with cybersecurity by placing an emphasis on the need to encrypt data regardless of geographic location. With such a measure in place, organizations can further defend against interception and unauthorized access while the data is in transit

Having a single shallow barrier defending an entire internal network lacks the means to sustain the need for encryption across all communications. Such a deficiency exposes the data to potential eavesdropping and man-in-the-middle attacks in an intercommunication network

Protecting your data and remaining compliant with regulatory frameworks becomes easier. Such a measure does bring in more refined control over the network's intelligence architecture, which heavily protects thhe trust boundaries

Project Information Slide

Zero Trust Comparison

3. Per-session access	
Users are given access to resources only for the duration of a session and after the session ends the access is removed. This reduces the time potential attackers can exploit a system once they get an unauthorized access to it	**Traditional models tend to provide longer-term access which can be more user-friendly, but, if the user’s credentials are compromised, it certainly poses a higher risk**
Greater control of resource usage along with reduced risk of unauthorized access make Zero Trust incredibly beneficial. With Per-session access, users are able to access resources only for the period these resources are actually needed, which in turn enhances the overall security	

Project Information Slide

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.

Project Information Slide

Zero Trust Model

Device Agent & Gateway

The Device Agent & Gateway model is the best fit for XYZ's current network challenges and security objectives for several reasons:

1. Comprehensive Device Management:
- Addressing Specific Security Challenges: XYZ has experienced recent security vulnerabilities that likely stem from unmanaged or poorly managed devices. The Device Agent & Gateway model ensures that all devices, whether they are corporate-owned or personal (BYOD), are continuously monitored and managed. This reduces the risk of unauthorized access and ensures that all devices comply with security policies.
- Alignment with Security Objectives: By implementing device agents, XYZ can enforce security policies at the device level, ensuring that only compliant and secure devices can access the network. This aligns with XYZ's goal of enhancing overall network security and reducing the attack surface.

2. Granular Access Control:
- Addressing Specific Security Challenges: The Device Agent & Gateway model provides granular access control, allowing XYZ to enforce context-aware access policies. This means that access is granted based on the device's security posture, user identity, and other contextual factors, reducing the risk of unauthorized access.
- Alignment with Security Objectives: This model supports XYZ's objective of implementing a robust zero-trust architecture by ensuring that access is continuously verified and that only trusted devices and users can access sensitive resources.

3.Enhanced Visibility and Control:
- Addressing Specific Security Challenges: The model offers enhanced visibility into device activities and network traffic, enabling XYZ to detect and respond to potential threats more effectively. This is crucial for addressing the recent security vulnerabilities and preventing future incidents.
- Alignment with Security Objectives: By providing detailed insights into device and user activities, the Device Agent & Gateway model supports XYZ's goal of maintaining a secure and compliant network environment.