

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.

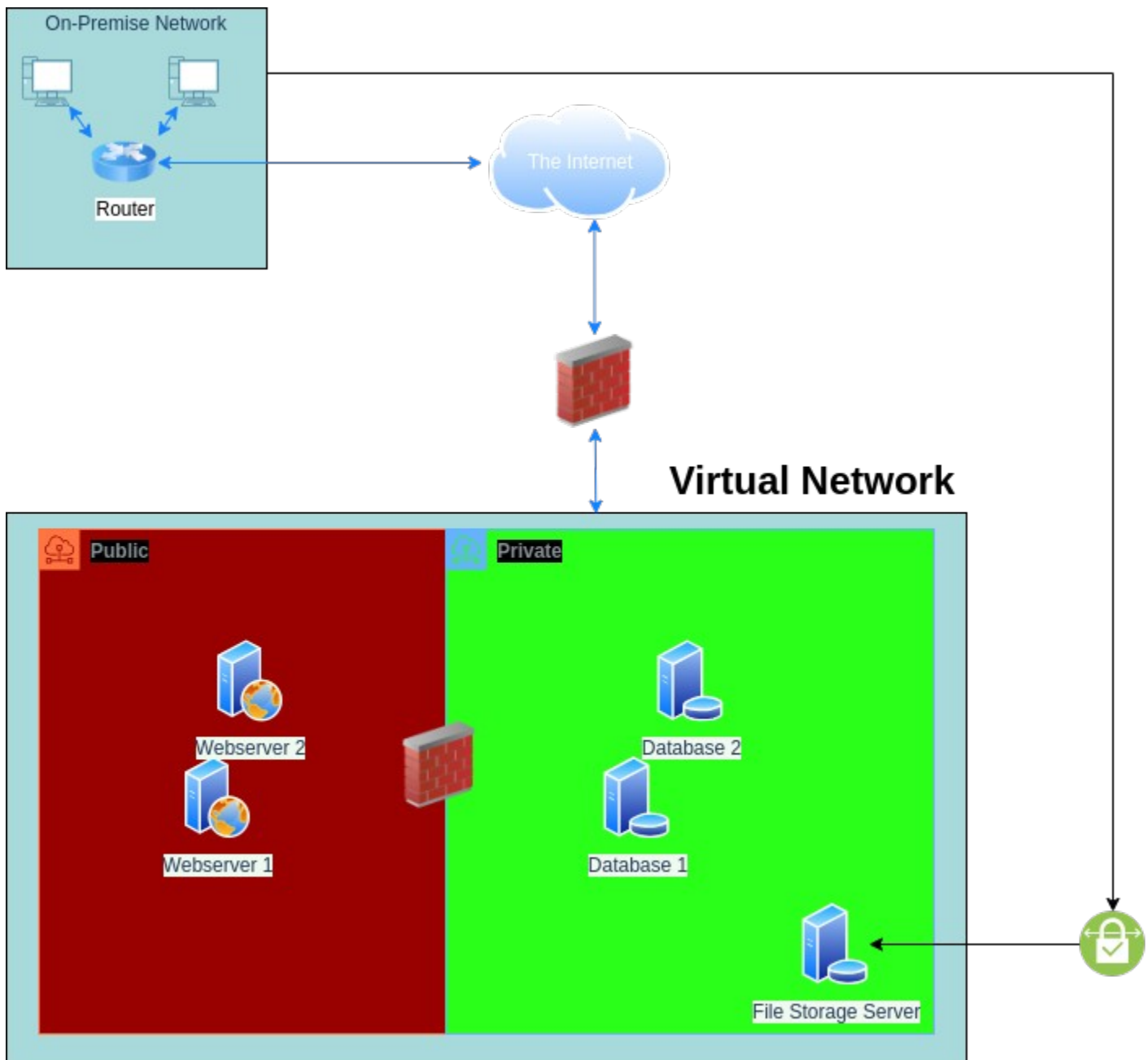
3. Lack of Access Control for File Storage Server

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

Microsoft Azure

Search resources, services, and docs (G+)

odl_user_259263@udaci...
UDACITY (UDACITYLABS.ONMIC...

Home > Virtual networks > DMZ

DMZ | Subnets

Virtual network

Search

+ Subnet + Gateway subnet Refresh Manage users Delete

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection

Search subnets

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group ↑↓	Route table ↑↓
default	10.0.0.0/24	-	251	-	-	-
Public-DMZ	10.0.1.0/24	-	251	-	Public-DMZ-NSG	-
Private-DMZ	10.0.2.0/24	-	251	-	Private-DMZ-NSG	-



Network Setup

Screenshot of the Internal Virtual Network with the subnet

Microsoft Azure

Search resources, services, and docs (G+/)

odl_user_259263@udaci...
UDACITY (UDACITYLABS.ONMIC...

Home > Internal-1715901662316 | Overview > Internal

Internal | Subnets

Virtual network

Search

+ Subnet + Gateway subnet Refresh Manage users Delete

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection

Search subnets

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group ↑↓	Route table ↑↓	
default	10.0.0.0/24	-	251	-	-	-	**
Internal-Subnet	10.0.1.0/24	-	251	-	-	-	**



Secure Routing Setup

Microsoft Azure

Search resources, services, and docs (G+I)

odl_user_259263@udaci...
UDACITY (UDACITYLABS.ONMIC...

Home > Network security groups > Private-DMZ-NSG

Private-DMZ-NSG | Inbound security rules

Network security group

Search

[Add](#) [Hide default rules](#) [Refresh](#) [Delete](#) [Give feedback](#)

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-MySQL-from-P...	3306	TCP	10.0.1.0/24	Any	Allow
110	Deny-All	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Automation

Microsoft Azure

Search resources, services, and docs (G+I)

odl_user_259263@udaci...
UDACITY (UDACITYLABS.ONMIC...

Home > Network security groups > Public-DMZ-NSG

Public-DMZ-NSG | Inbound security rules

Network security group

Search

[Add](#) [Hide default rules](#) [Refresh](#) [Delete](#) [Give feedback](#)

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-HTTP	80	TCP	Any	Any	Allow
110	Allow-HTTPS	443	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Automation



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

Microsoft Azure

Search resources, services, and docs (G+)

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20240516174703 | Overview >

Elk-Server

Virtual machine

Search

Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Connect
 - Connect
 - Bastion
- Networking
 - Network settings
 - Load balancing
 - Application security groups
 - Network manager

Essentials

Resource group (move): [entp-project-259263](#)

Status: Running

Location: East US

Subscription (move): [Udacity CloudLabs Sub - 26](#)

Subscription ID: c601b0a1-2f6f-4904-b50f-aa8d88855522

Operating system: Linux (ubuntu 20.04)

Size: Standard DS1 v2 (1 vcpu, 3.5 GiB memory)

Public IP address: [40.71.98.221](#)

Virtual network/subnet: [DMZ/Private-DMZ](#)

DNS name: [Not configured](#)

Health state: -

Time created: 5/16/2024, 11:54 PM UTC

Tags (edit): [Add tags](#)

Properties Monitoring Capabilities (7) Recommendations Tutorials

Virtual machine

Computer name: Elk-Server

Operating system: Linux (ubuntu 20.04)

Networking

Public IP address: [40.71.98.221](#) (Network interface [elk-server79](#))

Public IP address (IPv6): -

Private IP address: [10.0.2.4](#)

Microsoft Azure

Search resources, services, and docs (G+)

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20240516175616 | Overview >

Filebeat-VM

Virtual machine

Search

Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Connect
 - Connect
 - Bastion
- Networking
 - Network settings
 - Load balancing
 - Application security groups
 - Network manager

Essentials

Resource group (move): [entp-project-259263](#)

Status: Running

Location: East US

Subscription (move): [Udacity CloudLabs Sub - 26](#)

Subscription ID: c601b0a1-2f6f-4904-b50f-aa8d88855522

Operating system: Linux (ubuntu 20.04)

Size: Standard B1s (1 vcpu, 1 GiB memory)

Public IP address: [13.82.183.58](#)

Virtual network/subnet: [DMZ/Public-DMZ](#)

DNS name: [Not configured](#)

Health state: -

Time created: 5/16/2024, 11:58 PM UTC

Tags (edit): [Add tags](#)

Properties Monitoring Capabilities (7) Recommendations Tutorials

Virtual machine

Computer name: Filebeat-VM

Operating system: Linux (ubuntu 20.04)

Networking

Public IP address: [13.82.183.58](#) (Network interface [filebeat-vm855](#))

Public IP address (IPv6): -



Microsoft Azure

Search resources, services, and docs (G+)

odl_user_259263@udaci...
UDACITY (UDACITYLABS.ONMIC...

Home > Network security groups > Private-DMZ-NSG

Private-DMZ-NSG | Inbound security rules

Network security group

Search

+ Add Hide default rules Refresh Delete Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Automation

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Port == all

Protocol == all

Source == all

Destination == all

Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
<input type="checkbox"/> 100	Allow-MySQL-from-P...	3306	TCP	10.0.1.0/24	Any	<input checked="" type="checkbox"/> Allow
<input type="checkbox"/> 110	Deny-All	Any	Any	Any	Any	<input checked="" type="checkbox"/> Deny
<input type="checkbox"/> 120	Allow-SSH	22	TCP	Any	Any	<input checked="" type="checkbox"/> Allow
<input type="checkbox"/> 130	Allow-Kibana	5601	TCP	Any	Any	<input checked="" type="checkbox"/> Allow
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	<input checked="" type="checkbox"/> Allow
<input type="checkbox"/> 65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	<input checked="" type="checkbox"/> Allow
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any	Any	<input checked="" type="checkbox"/> Deny



Setup Monitoring

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

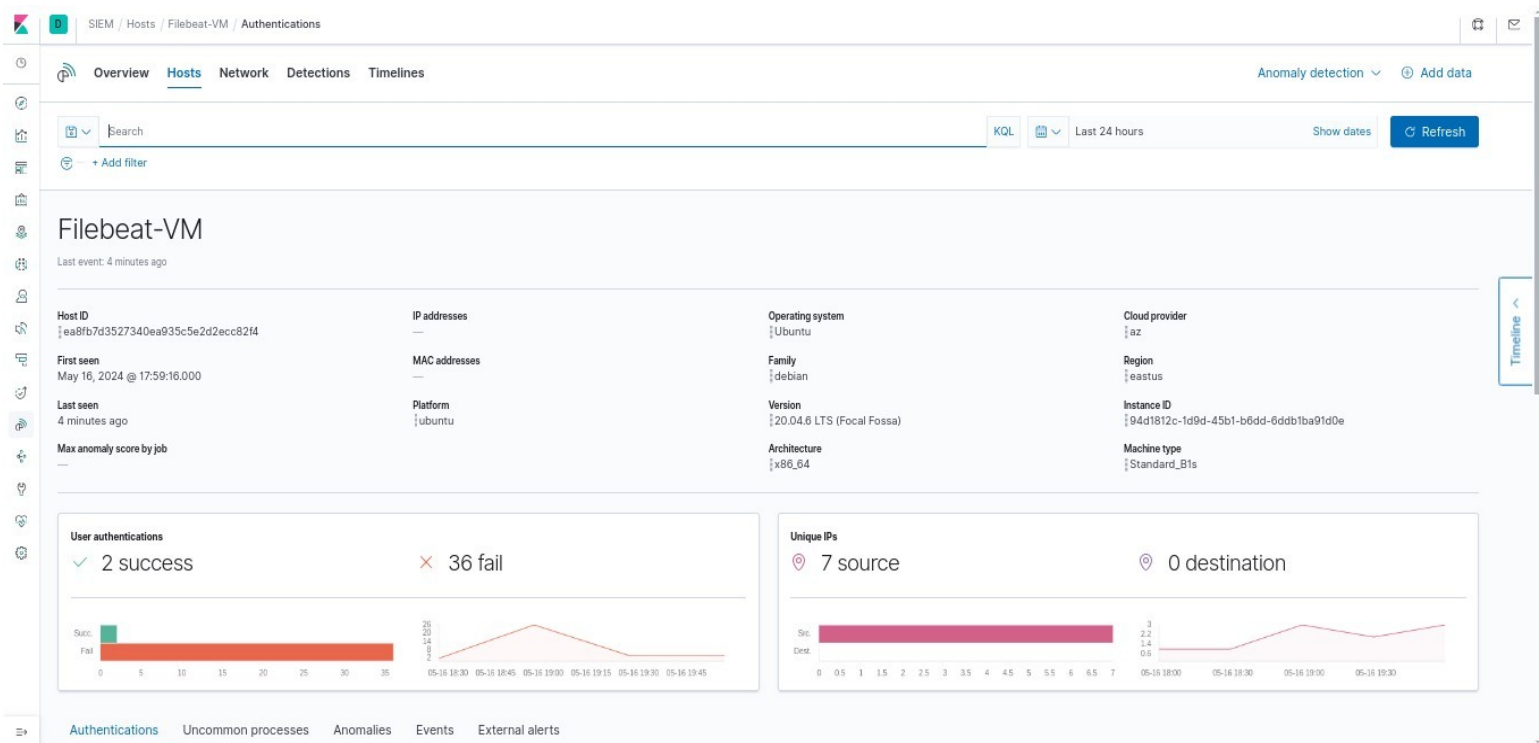
```
azuresuser@Filebeat-VM: /etc/filebeat
File Actions Edit View Help
azuresuser@Filebeat-VM:/etc/filebeat$ ls
fields.yml filebeat.reference.yml filebeat.yml modules.d
azuresuser@Filebeat-VM:/etc/filebeat$ sudo filebeat setup
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Loaded machine learning job configurations
Loaded ingest pipelines
azuresuser@Filebeat-VM:/etc/filebeat$ sudo service filebeat st
art
azuresuser@Filebeat-VM:/etc/filebeat$ systemctl status filebeat
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
   Loaded: loaded (/lib/systemd/system/filebeat.service; disabled; vendor preset: enabled)
   Active: active (running) since Fri 2024-05-17 02:02:14 UTC; 2min 53s ago
     Docs: https://www.elastic.co/products/beats/filebeat
    Main PID: 2738 (filebeat)
      Tasks: 8 (limit: 1002)
     Memory: 50.2M
    CGroup: /system.slice/filebeat.service
           └─2738 /usr/share/filebeat/bin/filebeat -e -c /etc/filebeat/filebeat.yml -path.home /usr/share/filebeat -path.config /etc/filebeat -path.data /var/lib/fib

May 17 02:02:14 Filebeat-VM filebeat[2738]: 2024-05-17T02:02:14.622Z      INFO      [index-management]      idxmgmt/std.go:437      Set settings.index.lifecyc>
May 17 02:02:14 Filebeat-VM filebeat[2738]: 2024-05-17T02:02:14.631Z      INFO      template/load.go:88      Template filebeat-7.4.0 already exists and will not>
May 17 02:02:14 Filebeat-VM filebeat[2738]: 2024-05-17T02:02:14.632Z      INFO      [index-management]      idxmgmt/std.go:289      Loaded index template.
May 17 02:02:14 Filebeat-VM filebeat[2738]: 2024-05-17T02:02:14.634Z      INFO      [index-management]      idxmgmt/std.go:300      Write alias successfully g>
May 17 02:02:14 Filebeat-VM filebeat[2738]: 2024-05-17T02:02:14.644Z      INFO      pipeline/output.go:105    Connection to backoff(elasticsearch(http://10.0.>
May 17 02:02:44 Filebeat-VM filebeat[2738]: 2024-05-17T02:02:44.237Z      INFO      [monitoring]      log/log.go:145      Non-zero metrics in the last 30s >
May 17 02:03:14 Filebeat-VM filebeat[2738]: 2024-05-17T02:03:14.236Z      INFO      [monitoring]      log/log.go:145      Non-zero metrics in the last 30s >
May 17 02:03:44 Filebeat-VM filebeat[2738]: 2024-05-17T02:03:44.236Z      INFO      [monitoring]      log/log.go:145      Non-zero metrics in the last 30s >
May 17 02:04:14 Filebeat-VM filebeat[2738]: 2024-05-17T02:04:14.236Z      INFO      [monitoring]      log/log.go:145      Non-zero metrics in the last 30s >
May 17 02:04:44 Filebeat-VM filebeat[2738]: 2024-05-17T02:04:44.236Z      INFO      [monitoring]      log/log.go:145      Non-zero metrics in the last 30s >
lines 1-20/20 (END)
```



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.