## Implement required level of perimeter security to meet organizational asset security requirements

* Identify all of the organization's external facing assets. This includes websites, servers, applications, and other devices that are accessible from the internet.
* Map out all of the communication channels between the organization's internal networks and external assets. This includes identifying all of the ports and protocols that are used.
* Implement firewalls at all external connectivity points. Configure the firewalls to restrict access to only authorized traffic and to block known malicious traffic.
* Implement strong access controls for all users, both internal and external. Use MFA for all users and implement least privilege access principles.
* Use encryption for all sensitive data, both in transit and at rest. This includes encrypting all data that is transmitted over the internet, such as web traffic and email. It also includes encrypting all data that is stored on servers and other devices.

## 

## 

## 

## 

## 

## 

## according to identified threats and vulnerabilities, assess and implement server and network hardening techniques and measures

* Identify their critical assets. This includes servers, applications, data, and other systems that are essential to the organization's operations.
* Assess the security posture of their servers and networks. This includes identifying any vulnerabilities that could be exploited by attackers.
* Implement appropriate hardening techniques and measures to address the identified vulnerabilities.
* Monitor their servers and networks for suspicious activity and respond to incidents promptly.

## 

## Implement secure authentication and user account controls to secure data integrity and Transmission

* Implementing a firewall at all external connectivity points. The firewall should be configured to restrict access to only authorized traffic and to block known malicious traffic.
* Implement a firewall at all external connectivity points. Configure the firewall to restrict access to only authorized traffic and to block known malicious traffic.
* Segment the network into different zones, such as DMZ, internal network, and guest network.
* Use strong authentication and authorization mechanisms for all network users.
* Encrypt all sensitive data in transit and at rest.
* Monitor network traffic for suspicious activity using IDS/IPS systems and network monitoring tools.
* Design a secure network architecture. This includes implementing a firewall at all external connectivity points and configuring it to restrict access to only authorized traffic. Organizations should also segment their network into different zones, such as DMZ, internal network, and guest network, and implement firewalls between each zone to further restrict access.
* Implement strong access controls. This includes using multi-factor authentication (MFA) for all users, both internal and external, and implementing least privilege access principles. Organizations should also regularly review their access control lists (ACLs) to ensure that only authorized users have access to sensitive data and systems.
* Use encryption. All sensitive data, both in transit and at rest, should be encrypted. This will help to protect data from unauthorized access even if it is compromised.
* Implement intrusion detection and prevention systems (IDS/IPS). IDS/IPS systems can help to identify and block malicious traffic before it reaches the network.
* Monitor network activity. Organizations should implement network monitoring solutions to detect suspicious activity, such as unauthorized login attempts or unusual traffic patterns.