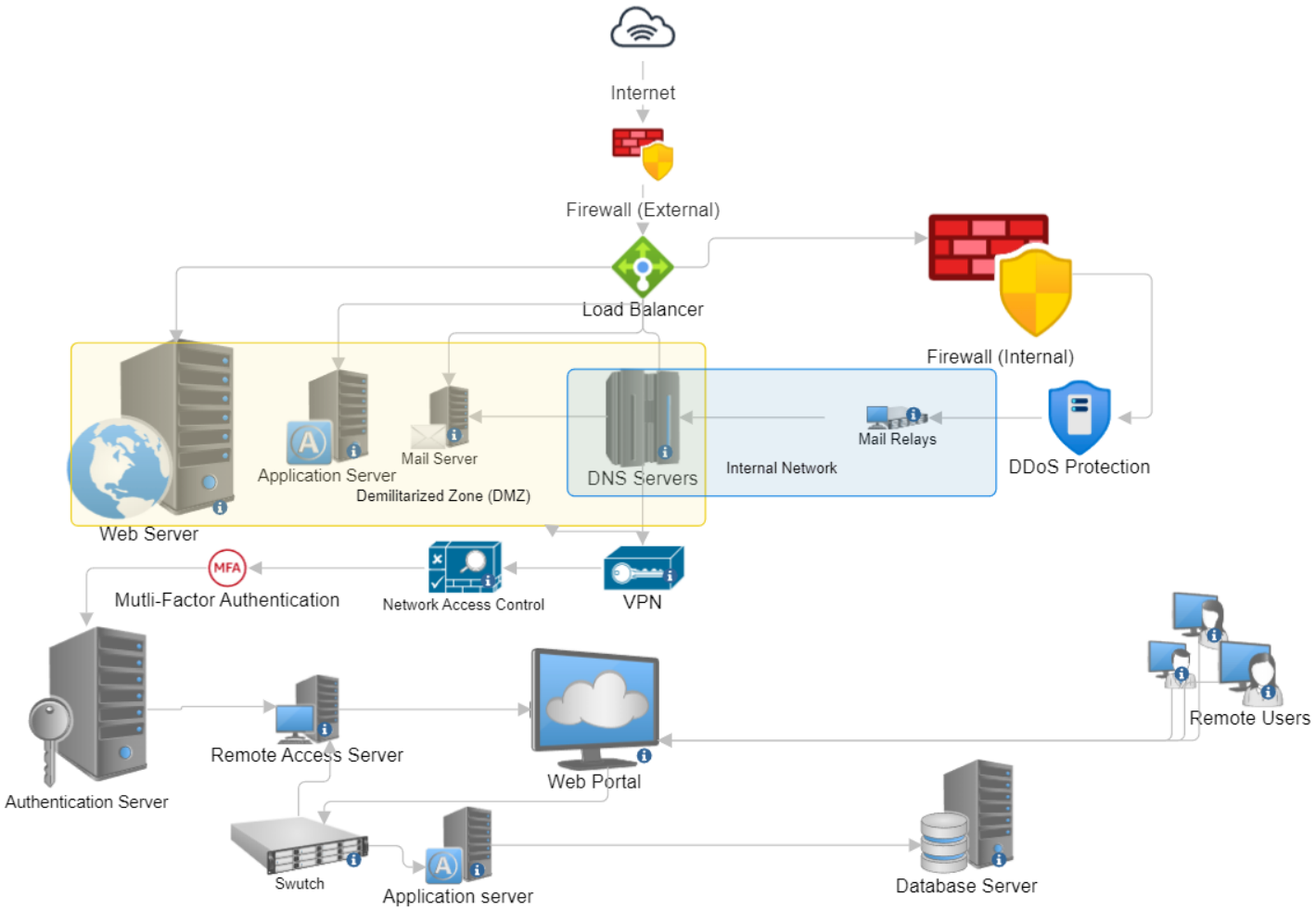
Assignment -1

Part-1

Data is a crucial and confidential asset of any organization. A secure network configuration is essential for organizations to handle sensitive and confidential information like the customer records and intellectual properties of the business organization. Such information stored in the databases and servers can be at risk of attacks, theft and has to be prevented from network outages and security incidents which can cause data breaches and break Confidentiality, integrity and availability thus disrupt the business. For secure remote work and smooth and reliable resource optimization many cyber security strategists have come up with the security network configurations. Here is one such network configuration which includes strategically placed multiple defenses at various levels of the data architecture of the organization.
The below secure network configuration in the diagram provides comprehensive security while maintaining efficient and reliable network operations:



Proposed Secure network Topology

- **Firewalls**: They are placed to create a robust secure perimeter. The external firewall which faces the internet, it is the first line of defense which filters the incoming traffic and blocks the potential threats while the second firewall which is the internal firewall is positioned within the network. It is added for the extra layer of protection by controlling the traffic between different network segments. The purpose of the firewalls is to prevent unauthorized access and protect the internal resources.
- **Load balancer**: This ensures availability and efficient resource utilization. It distributes the incoming network traffic evenly across the web server, application server, Dns server and mail servers. This will improve the user experience and also mitigate the risk of server overload or failures because of high volume traffic.
- **Web app and mail servers**: They are for services and applications. Web server serves the web content while app servers execute the application logic and mail servers handle email communications. These are connected to the load balancer which ensures that the load is distributed evenly without uninterrupted service and is available.
- **DNS servers**: These servers are responsible for converting domain names into their respective IP addresses. This is connected to load balancer to ensure efficient DNS resolution and uninterrupted service enhancing website accessibility and resilience against DNS related attacks.
- **Web application firewall**: It is positioned before the web server so that it can filter out the malicious request from incoming traffic and prevent the attacks which are incoming to the web servers like SQL injection cross site scripting.
- **Intrusion detection and prevention systems (IDS/IPS)**: that located in front of the application servers which filter out the anomalies or suspicious patterns of the malicious attacks this can ensure the integrity of the application layer.
- **Mail relay servers** facilitate the email communications between the incoming and outgoing mail servers services they give an extra layer of security to email traffic.
- **DdoS protection**: This is placed strategically in the network path which shields servers from DDOS attacks. They analyze the incoming traffic for anomalies and malicious behavior to mitigate the readers attacks to ensure the availability of data.
- **DMZ (Demilitarized zone)**: It is a semi-isolated network segment which will contain the services that can be accessed from the internet like the web servers and application servers, placing those servers in the DMZ enhances security by separating them from the internal network.
- **NAC/SIEM (Network Access Control and Security information event management)**: This ensures that only authorized devices gain network access.
- **Multi-factor authentication(MFA**): This is an additional layer of security for users authentication processes which enhances login security.
- **Authentication server**: This handles user authentication for remote access like through VPN gateways checking the validity of the credentials to gain access.
- **Remote users**: Who are often employees or partners have to be ensured that they can securely access the network resources outside the network that is handled through authentication and encryption.

- The **Web porta**l is a user-friendly interface for remote users to access internal resources and facilitate secure networks for remote work and collaboration.
- **VPN gateway**: It manages secure and encrypted tunnels for remote users ensuring confidentiality and integrity for the data transfer over the internet.
- **Application servers connected to web portal**: These servers host application logic and services internal to the organization and are responsible for delivering applications and services to end users
- **Database servers**: This stores and manages data critical to organization operations and then ensures availability, integrity and security of the information.

Security network configurations require defenses in depth and combinations of various security measures like the data protection policies that do traffic filtering, continuous monitoring for making data secure and reliable without redundancy. This configuration also supports remote access with strong authentication and encryption and enabling remote work capabilities providing confidentiality integrity and availability.

Part -2

In today's interconnected world computer security has become a vital importance. From recent security events we can emphasize the critical role it plays in the digital lives. This article aims to disclose the factual world of computer security for the audience, shredding a light on its significance, causes, prevention strategies and broader implications.

The recent security event involved a massive data breach at a prominent consumer council watchdog in Hong Kong. With hackers gaining unauthorized access to thousands of user accounts and threatening to expose personal information, resumes and credit card details in the dark web in return for ransome, highlights the vulnerabilities in the platform. This even sent shock waves through cyberspace stressing more on the need for robust security measurements.

The security event occurred due to a combination of factors including improper security protocols, lack of resources, human errors and disorganized huge data structures. Cyber criminals are becoming increasingly sophisticated probing for weakness and vulnerabilities in digital fortresses. In this case due to lack of proper secure firewalls, vulnerabilities were exploited leading to the breach.

Such events could have been prevented or the breach could have been mitigated by implementing proper security strategies involving strong authentication methods, regularly monitoring the software, updating security softwares and conducting vulnerability assessments frequently. Creating awareness among the users about online safety and multi-factor authentication implementations could have mitigated the attack.

Events like security breaches from beyond immediate consequences can raise ethical and societal issues. The breach compromised users' privacy and exposed them to identity theft and scams. Moreover it underscored the responsibility of corporations to protect the user data and the need for the governments to implement comprehensive data protection legislation.

The security breach events calls for responses from various stakeholders:

- **Public awareness:** The users must be made aware of their online presence prompting them to regularly change passwords and enable multi-factor authentications and educate them about the potential threats.
- **Policy makers**: They should enact and enforce more stringent data protection laws.
- **Corporations**: They must be held accountable for user data safeguarding and ensuring transparency in data handling.Company should be made aware that cyber security must be prioritized by investing in cutting edge technologies. They should conduct routine security audits and vulnerability assessments and they should take Swift actions to mitigate the attacks.
- **Media:** It also plays a crucial role in informing the public about the security risk and best practices. They should educate about cyber security incidents to raise awareness among them.

Computer security is a multifaceted field which affects every aspect of our digital lives. Recent security events are just a reminder of the importance of stringent security measures, ethical considerations and collective responsibility. By understanding these issues and taking actions we can navigate the digital world with greater confidence and security.