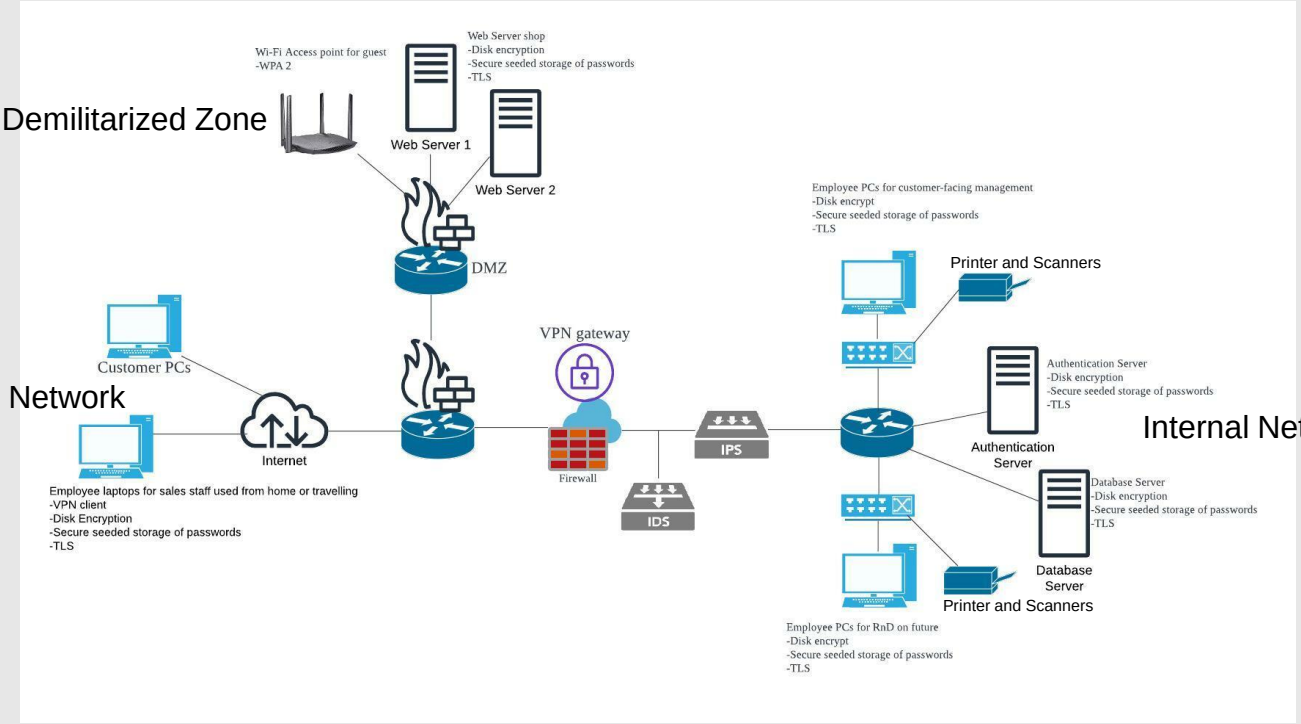
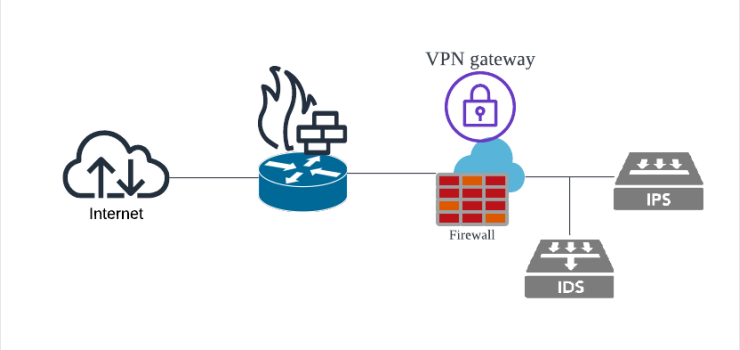
Security controls in a medium-sized company scenario

Teh Jia Xuan 32844700

Network Diagram



Before Access to Internal Network



Router (in-built firewall)
The router helps to forward data packets between networks. Firewall help to analyse incoming and outgoing packets that come from external networks based on security rules. Port numbers allowed to be accessed: FTP (20, 21), SSH (22), SMTP (25), DNS (53), HTTP (80), HTTPS (443), LDAP (389), RDP (3389)

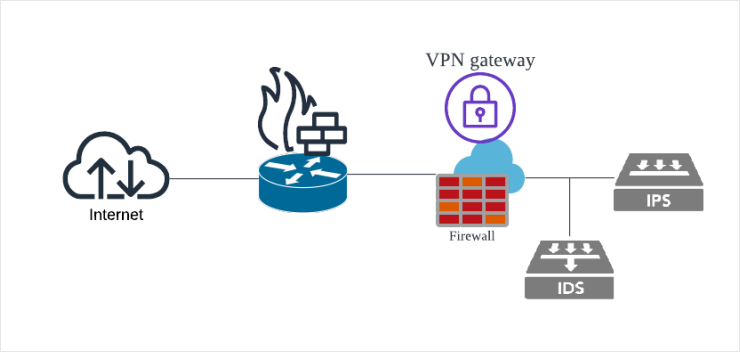
Firewall
Act as a first-line defence against external threats. Monitors and controls traffic that enters and outgoing based on security rules to protect the system from unauthorised access. Port numbers allowed to be accessed: FTP (20, 21), SSH (22), SMTP (25), DNS (53), HTTP (80), HTTPS (443), LDAP (389), RDP (3389)

VPN gateway
VPN gateway provides a secure, encrypted connection and enables the worker to access company resources while working from home or travelling securely.

Intrusion Detection System(IDS)
Generate an alert to the security administrator once it detects security threats

Intrusion Prevention System (IPS)
Block malicious activities based on a database of known attack

Before Access to Internal Network



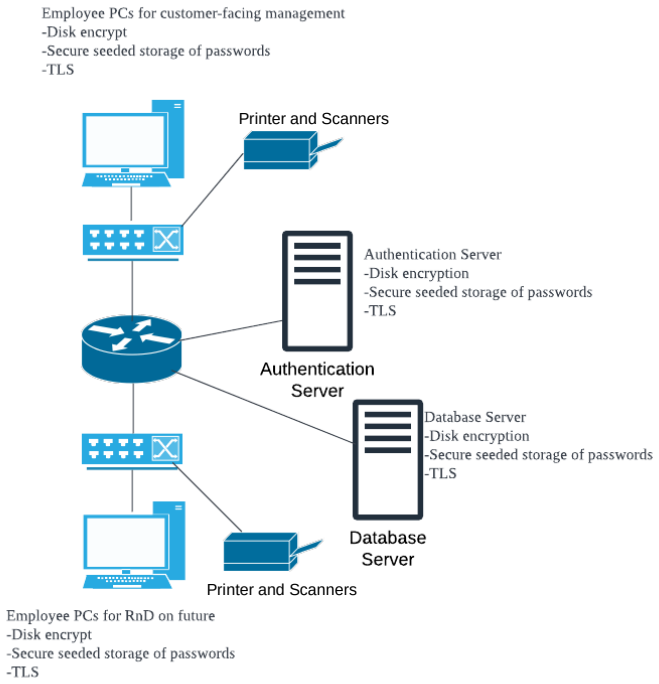
Router (in-built firewall)
The router in the middle transmits packets to the internal network and DMZ. A firewall is to monitor and controls incoming and outgoing packets.

VPN Gateway with firewalls
Employees can connect to VPN gateway when employee wants to access the internal network while travelling or working from home. Thus, a VPN gateway with firewalls can provide secure internal network access for their employee. Firewalls can protect the internal network from unauthorised access, while VPN gateway provides an encrypted tunnel for remote users to access the internal network. This can allow employees to work safely in public and prevent leaks of company information.

IDS
IDS is put in after the firewall to detect any malicious activity that the firewall has missed. When the attacker is able to bypass the firewall, IDS is able to alert security administrators. It also can reduce false alarms as the IDS only analyse packets that pass through the firewalls.

IPS
IPS is placed after IDS because IPS can block any detected threats based on the known attacks from the database and threats that are detected by IDS from entering the internal network

Internal Network



Disk Encryption

Protect computer-sensitive data by encrypting data into unreadable code to prevent unauthorised access. Even though the data is stolen, it can ensure the data won't be seen by others Some common disk encryption solutions like BitLocker etc.

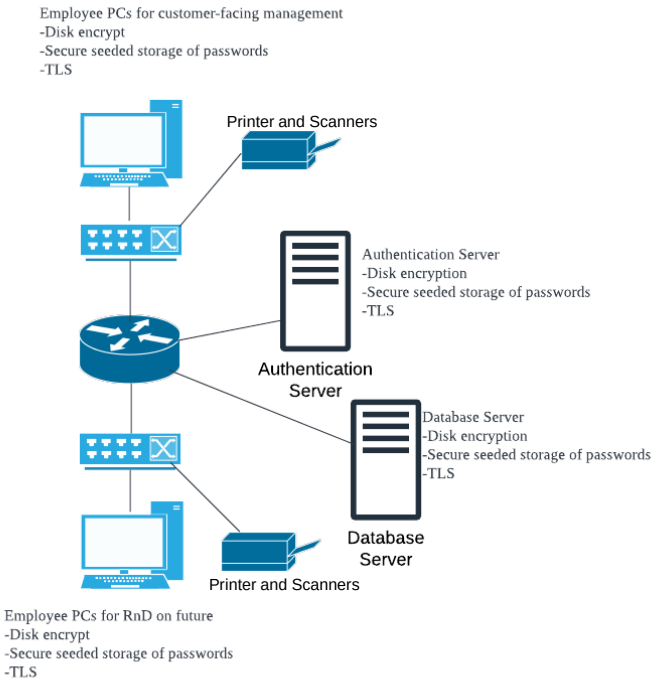
Secure seeded storage of password

Method of storing encrypted passwords to protect from unauthorised access or theft. It is done by combining password hash and salt value. The password hash and salt value are encrypted by the seed, which refers to a string of random characters. The seed is used to encrypt and decrypt passwords.

TLS

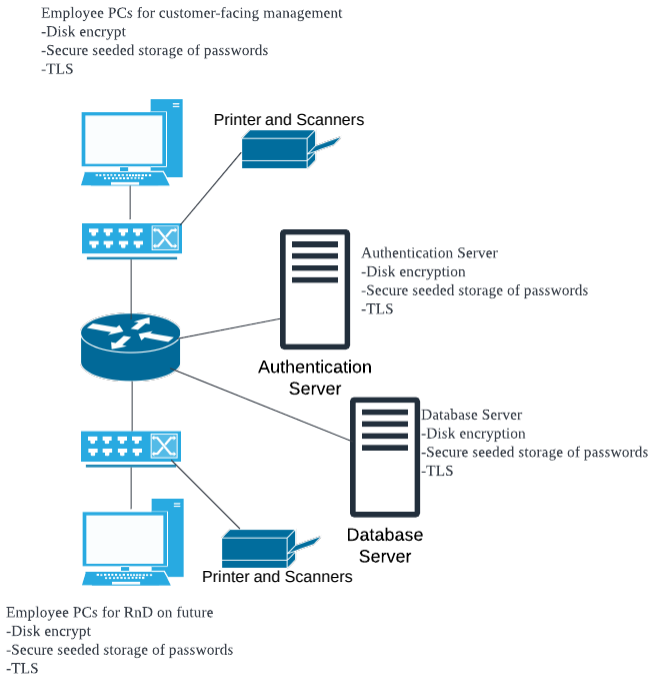
TLS ensure the data transmitted between two parties is kept confidential by using encryption algorithms. It also detects whether someone is modifying the data while it is transmitting. Thus, it also helps to ensure that both parties receive accurate data.

Internal Network



(LiveHome 3D, 2020)

Internal Network



Router and Switch

The router and switch help to forward data packets between networks and devices.

Authentication Server

Place in the internal network, as it is protected from unauthorised access from outside the network.

Customer Database Server

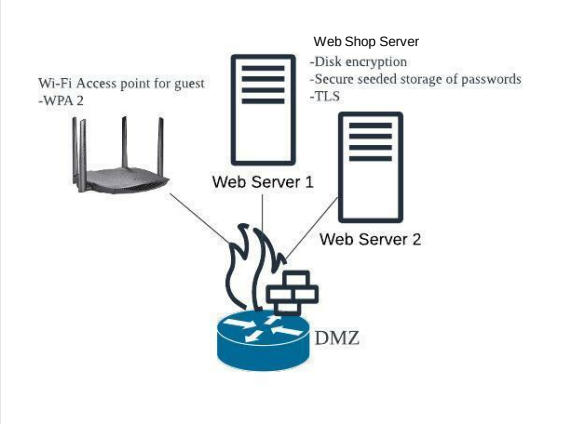
The customer database server is very important. Thus, I place it in the internal network to protect it from unauthorised access, and it can take advantage of other security measures before accessing the internal internet.

Besides that, every employee must verify their identity by using an authentication server, and the authentication server will return a ticket to access to customer database server. Every ticket has a different level of permission to the customer database server depending on the role of that employee.

Employee PCs and printer and scanner

RnD and customer-facing management pc and printer are separate as RnD is a highly classified department, as we don't want other competitors to know about our upcoming products. Thus, only the RnD department can access RnD information. This can prevent information leaks to other departments and prevent human errors.

Demilitarized Zone (DMZ)



(LiveHome 3D, 2020)

Router with firewalls

Monitors and controls packets from the network traffic. It is a barrier between DMZ and external networks to protect unauthorised access. Port numbers allowed to be accessed: FTP (20, 21), SSH (22), SMTP (25), DNS (53), HTTP (80), HTTPS (443), LDAP (389), RDP (3389)

Web Server Shop

Disk encryption is installed to encrypt the data in the server. To prevent the leak of information if hackers have access to the server.

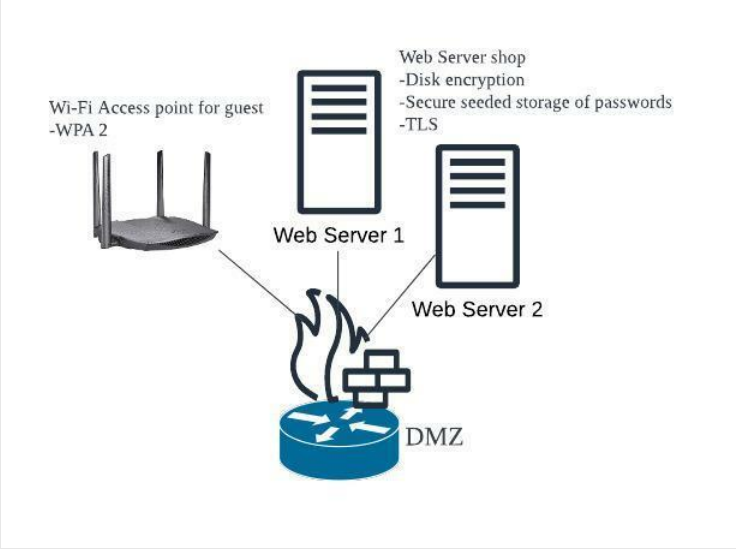
Secure seeded storage of passwords is installed to prevent hackers from accessing the server even if they got the hash password and salt value of the server.

TLS is applied to servers to ensure integrity and security when servers communicate with the customer's browser

Wi-Fi Access point for guest

WPA 2 is installed to provide encryption and authentication. Besides that, it ensures the integrity of the data transmitted.

Demilitarized Zone



Web Servers Shop
Web servers are located at DMZ because we want the public to access web servers without accessing our internal network. Hence it is located at DMZ to prevent the public from accessing the internal network.

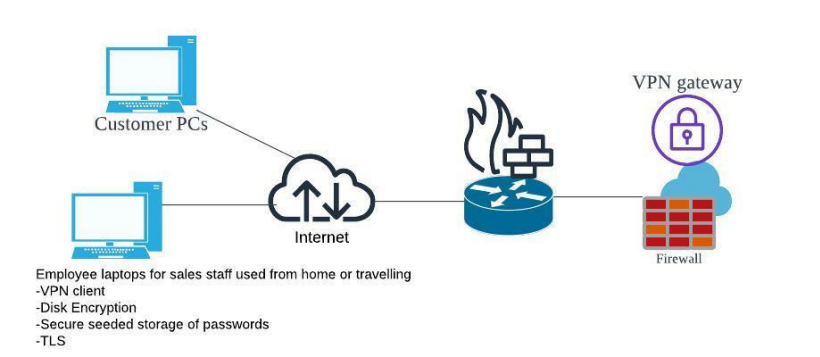
Two servers for the web shop, and 1 acts as a backup server. Whenever one of the servers is down, another web server will back up to ensure the user can continue to browse.

Furthermore, if One of the server's data gets corrupted, another server won't get affected.

Moreover, If one of the servers becomes overwhelmed, another server helps to balance the load.

Wi-FI Access point for guest
WPA 2 protect the privacy and integrity of data transmitted over the network. The access point placed in DMZ is because we wanted guests to access our Wi-FI without accessing our internal network.

External Network



Disk Encryption

protect computer-sensitive data by encrypting data into unreadable code to prevent unauthorised access. Even though the data is stolen, it can ensure the data won't be seen by others Some common disk encryption solutions like BitLocker etc

Secure seeded storage of password

Method of storing encrypted passwords to protect from unauthorised access or theft. It is done by combining password hash and salt value. The password hash and salt value are encrypted by the seed, which refers to a string of random characters. The seed is used to encrypt and decrypt passwords.

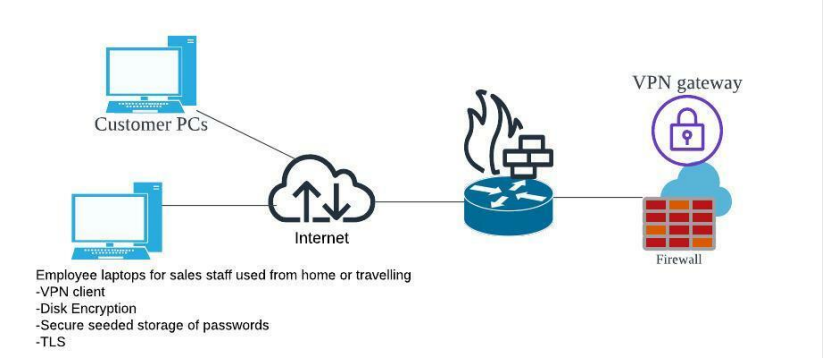
TLS

TLS ensure the data transmitted between two parties is kept confidential by using encryption algorithms. It also detects whether someone is modifying the data while it is transmitting. Thus, it also helps to ensure that both parties receive accurate data.

VPN Client

Enable the user to establish a connection to the VPN gateway. It provides secure and private access to the internet by encrypting the data transmitted between the VPN server and the device

External Network



Employee PCs for travelling and working from home
VPN client is installed to enable employees to access the internal internet while travelling or working from home. It also ensures that no one can sniff company information while employees are working in public.

Disk encryption is installed to encrypt the data in the computer. To prevent leak of information if computer or data has been stolen.

Secure seeded storage of passwords is installed to prevent hackers from access to employees' computers even if they got the hash password and salt value of the employee's computers.

TLS is applied to computers to ensure integrity and security when employees communicate with other parties.

References

Chkadmin. (2022, March 8). *IDs vs IPS*. Check Point Software. Retrieved from, https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/ids-vs-ips/

Gillis, A. S. (2022, October 18). *What is full-disk encryption? – definition from techtarget.com*. WhatIs.com. Retrieved from, https://www.techtarget.com/whatis/definition/full-disk-encryption-FDE

Manico, J. (2022, September 15). *Secure storage of passwords in your application*. Cobalt. Retrieved from, https://www.cobalt.io/blog/secure-storage-of-passwords-in-your-application

CISA. (n.d.). *Security tip (ST04-004)*. Retrieved from, https://www.cisa.gov/uscert/ncas/tips/ST04-004#:~:text=Firewalls%20provide%20protection%20against%20outside,or%20network%20via%20the%20internet.

Barracuda Networks. (2022, October 21). *VPN client*. Retrieved from, https://www.barracuda.com/support/glossary/vpn-client

Fortinet. (n.d.). *What is a DMZ and why would you use it?* Retrieved from, https://www.fortinet.com/resources/cyberglossary/what-is-dmz

References

Techopedia.com. (n.d.). *What is a VPN gateway? - definition from Techopedia*. Retrieved from, https://www.techopedia.com/definition/30755/vpn-gateway#:~:text=A%20VPN%20gateway%20is%20a,to%20connect%20multiple%20VPNs%20together.

CloudFlare(n.d.). *What is transport layer security? | TLS protocol |* Retrieved from, https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/