

Network Security and Cryptography

Wonder Telecoms

Prepared by
Amaan Al Mir

Table of Contents

Cover	1
Table of Contents	2
Task 1 – Risk Assessment – 15 Marks	4
a. Top 5 Information Assets	4
1. Customer Data	4
2. Company Files and Documents	4
3. Internal Network	5
4. E-commerce Website	5
5. File Server	5
b. Threats to Company's Assets	7
Task 2 – Risk Control – 35 Marks	9
a. Security Implementations	9
1. Threat: Unauthorized access	9
2. Threat: Malware infection	10
3. Threat: Data loss	10
4. Threat: Server Failure	11
5. Threat: Data theft	12
6. Threat: Cyberattack	13
b. Protecting E-Commerce Website	15
1. Vulnerabilities	15
2. Security Recommendations	17
3. Email Security	18

Task 3 – Securing the Network – 30 Marks.....	19
a. Virtual Private Network (VPN)	19
Key Features of VPN.....	20
Suitable types of VPN Connections.....	21
b. Firewalls and DMZ	25
Updated Network Infrastructure.....	27
c. Improvement of Internal FTP Server	28
Task 4 – Security Maintenance – 10 Marks.....	31
Task 5 – Reflective Commentary – 10 Marks.....	33
References	34

Task 1 – Risk Assessment – 15 Marks

a. Top 5 Information Assets

These are the five most important information assets for Wonder Telecoms:

1. Customer Data

This is company's greatest asset. It holds personal information of customers such as their names, addresses, email addresses, passwords and credit card details. This data is important to the company's business and its loss could cause serious damage to company's reputation and financial status.

2. Company Files and Documents

These include documents like financial reports, marketing plans, backup data, and other confidential information. Documents that are required for company's day-to-day operations. Unauthorized access, modification, or loss of this data could affect company's operations.

3. Internal Network

The company's internal network architecture is also important to protect as it holds their network details such as their routers, devices and softwares they're using. This information must be kept confidential. Plus, remote employees have access to the company's internal network via the Remote Desktop Protocol (RDP). The company must make sure that its network is secure from unauthorized access to prevent data theft, breaches, or loss of confidential information.

4. E-commerce Website

Wonder Telecoms' e-commerce website is the main platform for customers to manage their TV subscriptions. The website uses many open-source softwares like Apache HTTP Server, Magento Commerce, Oracle GlassFish Server, and MariaDB. These programs are often targeted by hackers, making the website a vulnerable to cyberattacks.

5. File Server

Following the fire incident, an internal file server was installed to share company files and documents with employees. This

server is accessible to all employees, and it is essential to make sure that the data on this server is secure and only accessible to authorized personnel.

In conclusion, these five assets are the most important for Wonder Telecoms. The protection of these assets is essential for the continuity of the company's business operations, and any breach or loss of data could have severe consequences.

(Barker, 2003)

b. Threats to Company's Assets

Asset	Threat	CIA?	Likelihood	Impact	Risk
Customer Data	Unauthorized access	C	High	High	Very High
	Data theft	C, I	Low	High	Medium
	Data loss	A	Medium	Medium	Medium
Company's Files and Documents	Unauthorized access	C	Medium	High	High
	Data theft	C, I	Low	High	Medium
	Data loss	A	Medium	Medium	Medium
Company's Internal Network	Unauthorized access	C	Medium	Medium	Medium
	Server failure	A	High	High	Very High
E-commerce Website	Cyberattack	CIA	High	High	Very High
	Server failure	A	High	High	Very High
	Data loss	I, A	Low	Medium	Low
File Server	Unauthorized access	C	Medium	High	High
	Malware or virus infection	A	Medium	Medium	Medium
	Server failure	A	Low	High	Medium

The likelihood and impact of threats in the above table is considered using the below definitions:

	Likelihood	Impact
Low	Less than once per year	Inconvenience may affect operation for a day or two
Medium	Once per year to once per week	The operation may be impacted for over a week, loss of customers
High	Several times a week	Company may not survive – lost reputation and customers

The risk column is calculated by using the below matrix:

		Impact		
		Low	Medium	High
Likelihood	Low	Very Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Very High

Task 2 – Risk Control - 35 Marks

a. Security Implementations

1. Threat: Unauthorized access

To reduce the risk of unauthorized access to customer and company's data, Wonder Telecoms should implement strong user authentication systems. This can be achieved by implementing two-factor authentication, using strong passwords, and restricting access to sensitive data to authorized personnel only. Encrypting the data can also provide an additional layer of security.

(Stallings, 2010)

Alternative countermeasures to reduce the risk of unauthorized access include implementing intrusion detection and prevention systems (IDS/IPS) and implementing network segmentation. IDS/IPS can detect and prevent unauthorized access, while network segmentation can limit the scope of potential breaches.

(Scambray, et al., 2000)

2. Threat: Malware infection

To reduce the risk of malware infection, Wonder Telecoms should install antivirus softwares on their devices and network. Regular system scans can also help identify and protect their data from potential threats that could be caused by malwares and other viruses.

(Stallings, 2010)

Alternative countermeasures to reduce the risk of malware infection includes implementing email and web filtering. Email filtering can prevent employees from accidentally opening malicious attachments or clicking on malicious links, while web filtering can prevent employees from accessing potentially harmful websites.

(Tracy, et al., 2007)

3. Threat: Data loss

To reduce the risk of data loss, Wonder Telecoms should implement a robust data backup and recovery plan. This plan should include regular backups to both local storage and online database or off-site storage, as well as a process for testing

backups to ensure they can be restored in the event of a failure. They should also make sure that all backups are encrypted and secure, with access restricted to authorized personnel only.

(Stallings, 2010)

Alternative countermeasures to reduce the risk includes the use of RAID (redundant array of independent disks) or cloud storage to increase data availability and redundancy. This will help to prevent data loss due to hardware failure, cyberattacks, and other threats.

(Scambray, et al., 2000)

4. Threat: Server Failure

To reduce the risk of server failure, Wonder Telecoms should implement redundancy and failover systems to make sure that critical services remain operational even in the event of a server failure. Additionally, regular maintenance and testing can help to identify and prevent potential server failures before they occur.

(Stallings, 2010)

Alternative countermeasures to mitigate the risk of server failure include implementing load balancing to distribute traffic across multiple servers, as well as implementing disaster recovery plans to make sure that critical data and services can be quickly restored in the event of a server failure. Additionally, implementing monitoring systems to detect and alert IT staff of server issues can help to quickly identify and solve failures.

(Scambray, et al., 2000)

5. Threat: Data theft

To reduce the risk of data theft, Wonder Telecoms should implement access controls to make sure that only authorized personnel have access to sensitive data. Encrypting the data can also help to hide and protect the data.

(Stallings, 2010)

Alternative countermeasures to mitigate the risk of data theft include implementing data loss prevention (DLP) software to monitor and control sensitive data within the network, as well as implementing network segmentation to limit the spread of a breach and ensure that sensitive data is protected even if a part of the network is compromised. Additionally, implementing

intrusion detection and prevention systems (IDS/IPS) can help to detect and prevent data theft attempts.

(Scambray, et al., 2000)

6. Threat: Cyberattack

To reduce the risk of cyberattacks, Wonder Telecoms can implement the following security measures:

- Install and regularly update anti-virus, anti-malware, and anti-spyware softwares on all devices.
- Implement a robust firewall to protect against unauthorized access and intrusion attempts.
- Conduct regular tests to find flaw in the system and fix them before they can be exploited.
- Implement two-factor authentication to add an extra layer of security for customer and staff accounts.
- Train employees on how to identify and avoid phishing scams and other tactics used in cyberattacks.

Alternative countermeasures:

- Implementing network segmentation to prevent the spread of a cyberattack across the entire network.
- Implementing a recovery plan to minimize the damage caused by a successful cyberattack and to quickly restore them.
- Regularly back up data and store them offsite or in cloud to prevent data theft in the event of a cyberattack.
- Regularly conduct cybersecurity audits to identify vulnerabilities and fix them.
- Enable email and web filtering to prevent employee from opening malicious attachments and links.

(Scambray, et al., 2000)

b. Protecting E-Commerce Website

1. Vulnerabilities

a. Apache HTTP Server

Apache HTTP Server is an open-source web server that is used by Wonder Telecoms to host e-commerce website online. The following vulnerabilities are known to affect Apache HTTP Server 2.4.50:

- [CVE-2016-8740](#): An issue in the HTTP/2 implementation in Apache HTTP Server can lead to a heap-buffer overflow. This could be exploited by a remote attacker trying to execute harmful code on the system.

(NIST, 2016)

- [CVE-2023-25690](#): An issue that allows HTTP request smuggling attack. An attacker can exploit this vulnerability to read sensitive data on the system.

(NIST, 2023)

b. Magento Commerce

The following vulnerability affects Magento Commerce 2.4.2:

- [CVE-2021-36043](#): An issue affected by a SSRF vulnerability in the dotmailer extension. Anyone with admin privileges could abuse this to attack using remote code execution.

(NIST, 2021)

c. MariaDB

MariaDB is a popular open-source database management system. The following vulnerability affects MariaDB 10.2:

- [CVE-2021-27928](#): An issue in MariaDB Server that can lead to an SQL injection attack. This could allow an attacker to execute harmful SQL statements on the system.

2. Security Recommendations

To fix the vulnerabilities affecting Apache HTTP Server, Wonder Telecoms should upgrade to the latest version of the software. Additionally, they should configure Apache HTTP Server to use a secure configuration by enabling Secure Socket Layer/Transport Layer Security (SSL/TLS), disabling unnecessary modules, and implementing strict access controls.

(Thomas, 2000)

To fix the remote code execution vulnerability affecting Magento Commerce, Wonder Telecoms should upgrade to the latest version of the software. They should also make sure that all patches and security updates are applied in a timely manner.

To fix the SQL injection vulnerability affecting MariaDB, Wonder Telecoms should upgrade to the latest version of the software. They should also implement secure coding practices to prevent SQL injection, such as input validation and parameterized queries. They should also implement access control feature to limit the use to authorize personnel only.

(Scambray, et al., 2000)

3. Email Security

To prevent staff from sending incorrect or faulty emails to customers, Wonder Telecoms should implement the following measures:

- a. Encryption: Wonder Telecoms should make sure that all their emails are encrypted. A VPN can be installed to encrypt the emails sent through the Internet. It can help encrypt the entire mail including header details like sender's and receiver's email addresses, subject, and body.

(Tracy, et al., 2007)

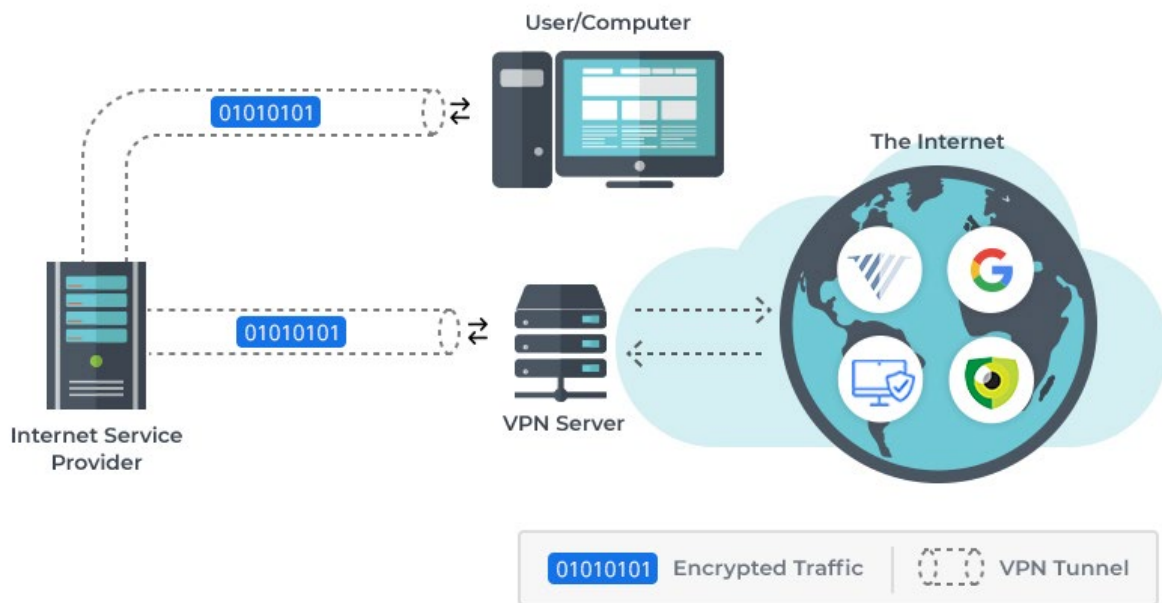
- b. Employee training: Wonder Telecoms should provide regular training and education to their employees on data protection and cybersecurity practices. This should include training on how to handle and securely send sensitive information.

- c. Access Controls: Wonder Telecoms should implement strict access controls for their email distribution lists, ensuring that only authorized personnel have access to these lists. They should also implement email validation mechanisms to prevent errors in email addresses.

(Tracy, et al., 2007)

Task 3 – Securing the Network – 30 Marks

a. Virtual Private Network (VPN)



A VPN, or Virtual Private Network, help to build a secure and encrypted connection between two or more devices over public internet. It creates a secure tunnel to protect the data from being altered or read by unauthorized users.

(Tanenbaum, 2002)

Key Features of VPN

1. **Authentication:** This verifies the data sent through a VPN.
2. **Access Control:** This prevents unauthorized users from gaining access to the network.
3. **Confidentiality:** This helps to keep the data a secret by not letting anyone read or copy it.
4. **Integrity:** This make sures that the data cannot be modified.

In the scenario, a VPN can be installed to allow remote employees to securely connect to the company's internal network from their homes via public internet. This way the company's data will be encrypted and secured, from being altered or read by unauthorized individuals and other spyware programs.

(Tanenbaum, 2002)

Suitable types of VPN Connections

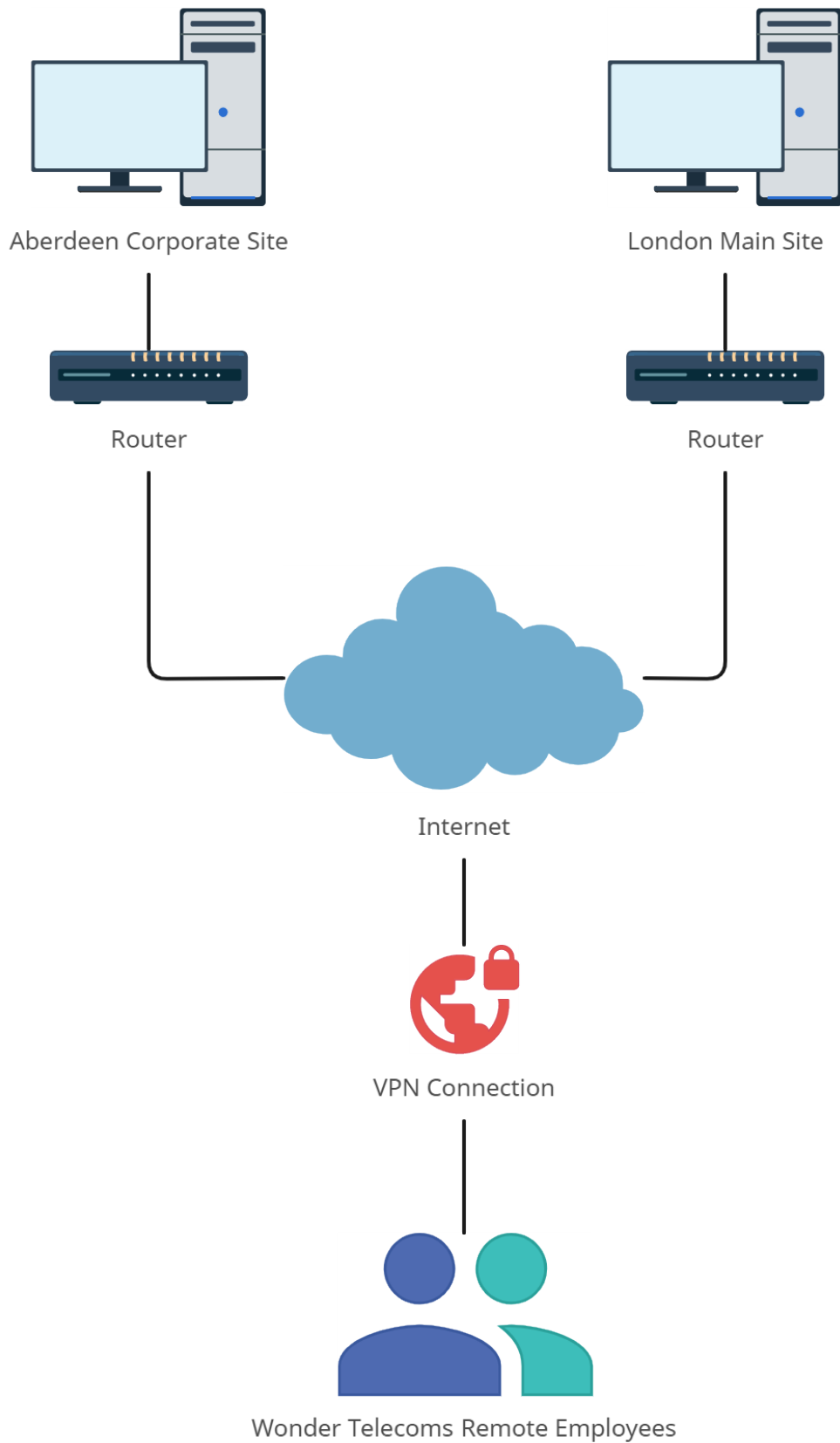
The suitable types of VPN connection options that are appropriate for the scenario are:

1. Remote Access VPN

This type of VPN connections are encrypted connections between corporate networks and remote users. This will help remote employees connect to the company's internal network from their homes or any other public internet access points. The Remote Access VPN connection can provide secure access to the company's data while maintaining the confidentiality and integrity of the data.

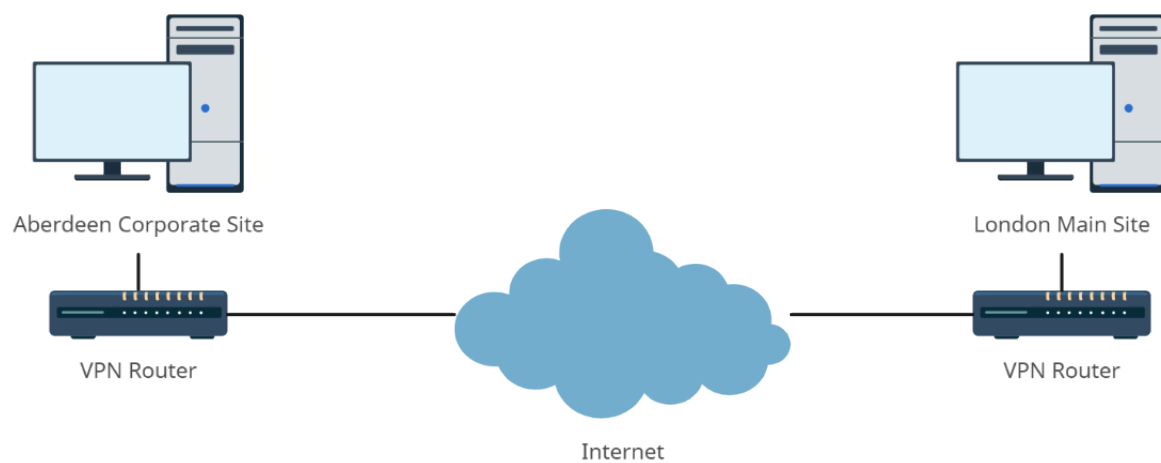
(Tanenbaum, 2002)

Please see the diagram on the next page for better understanding.



2. Intranet VPN

Intranet or Site-to-Site VPN connects two or more networks from different locations. For example, the London and Aberdeen sites.



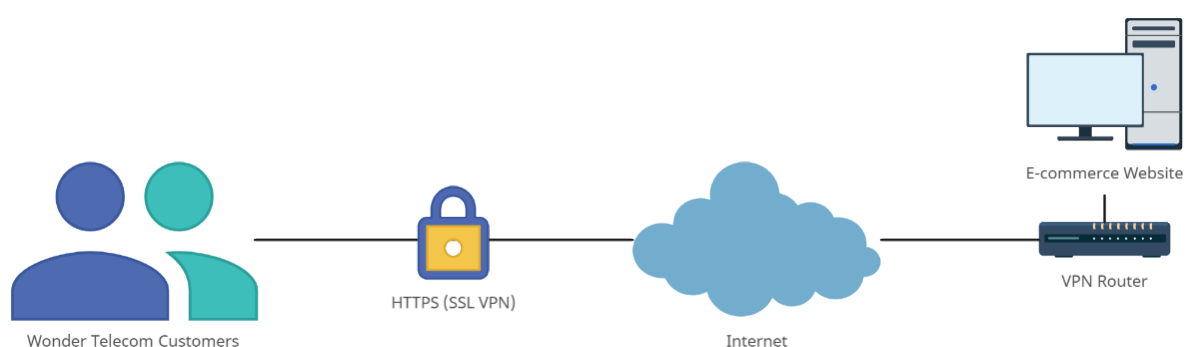
This type of VPN connection can be used to securely connect the two sites and ensure that all employees have access to the network resources.

3. Extranet VPN

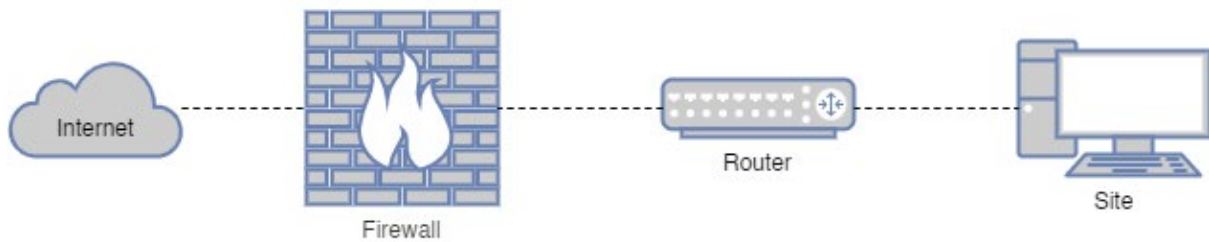
Extranet or Client-to-Site VPN enables individual devices, such as laptops and mobiles, to connect to the company's internal network from any location with internet access. This connection can be used to provide secure access to the company's resources while maintaining the confidentiality and integrity of the data.

(Tanenbaum, 2002)

This connection can also be used to allow customer access the company's e-commerce website using encrypted SSL certificate.



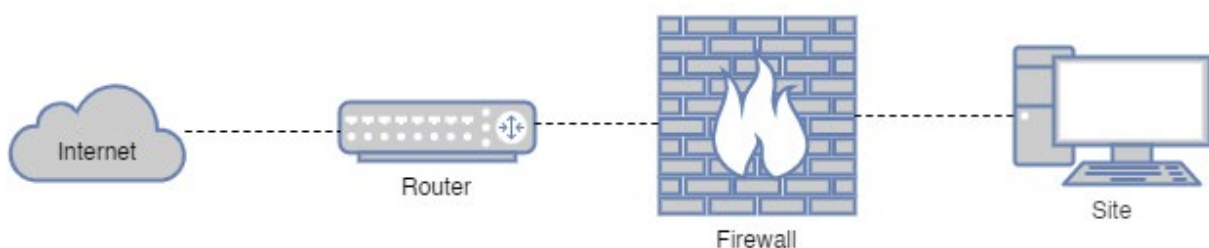
b. Firewalls and DMZ



A firewall is a primary defense in network security. It's like a barrier that controls outgoing and incoming traffic between the external and internal network. Firewalls protect against unauthorized access to the network. It also helps protect against malicious attacks and unwanted network traffic.

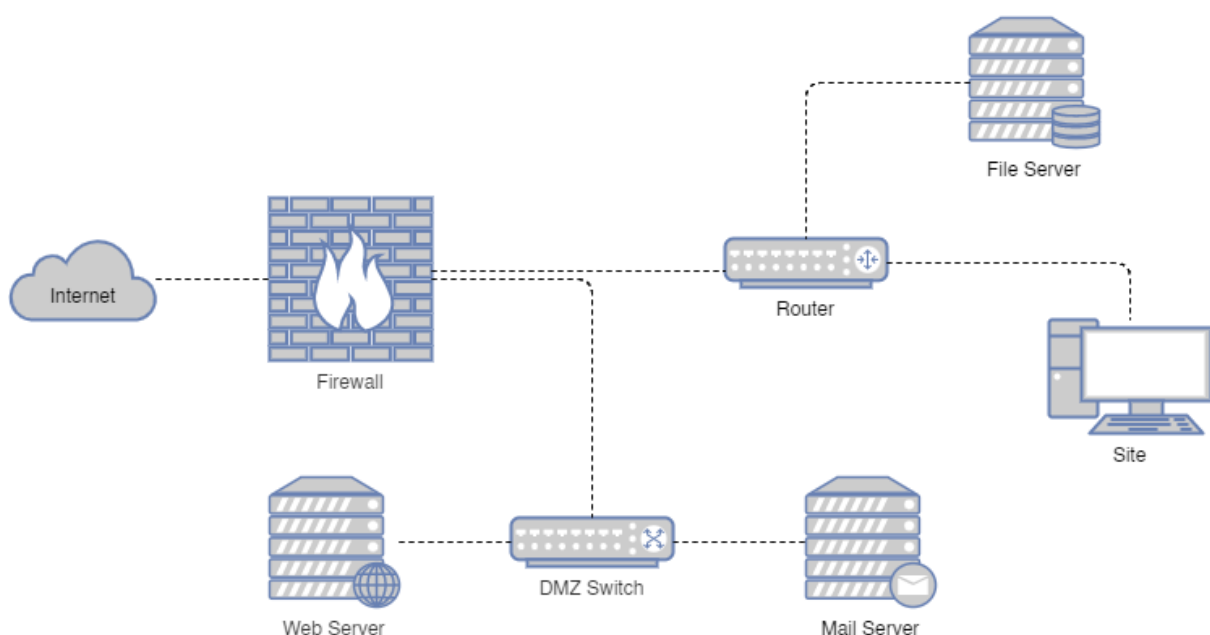
(Zwicky, et al., 2000)

Firewalls can be installed on both router and computer. Software firewall can only protect one device while the router firewall can help protect the entire network. It is up to network admin to decide where they want to install. They may choose to install on both.



A DMZ (Demilitarized Zone) is part of internal network but separate from it. It acts as a buffer zone to host public-facing servers, like Web and Email servers, that need to be accessible from the internet while keeping the internal network protected.

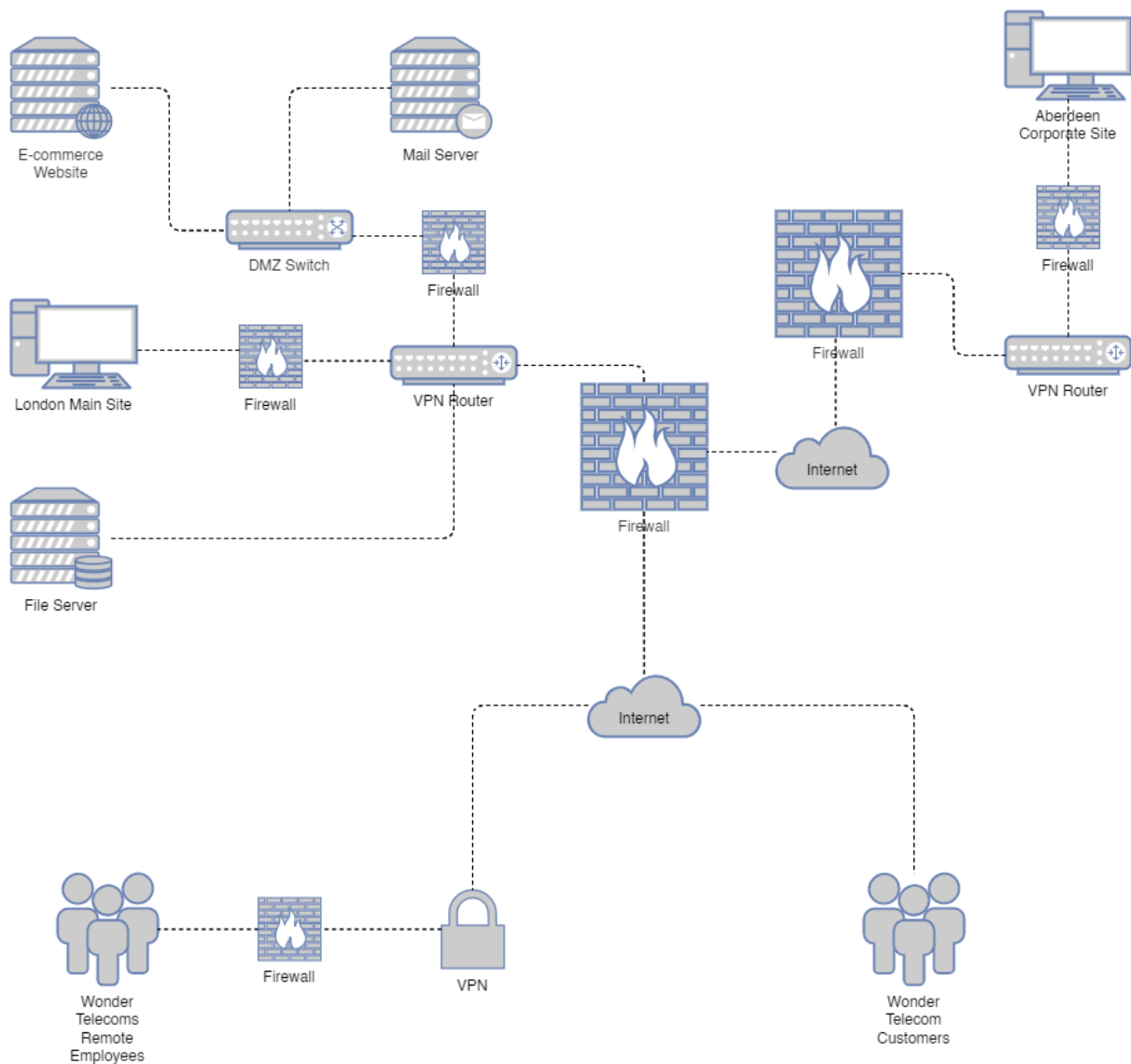
(Zwicky, et al., 2000)



By placing the e-commerce web server and email server in the DMZ, Wonder Telecoms can add an extra layer of security and mitigate the risk of direct access to their internal network.

Updated Network Infrastructure

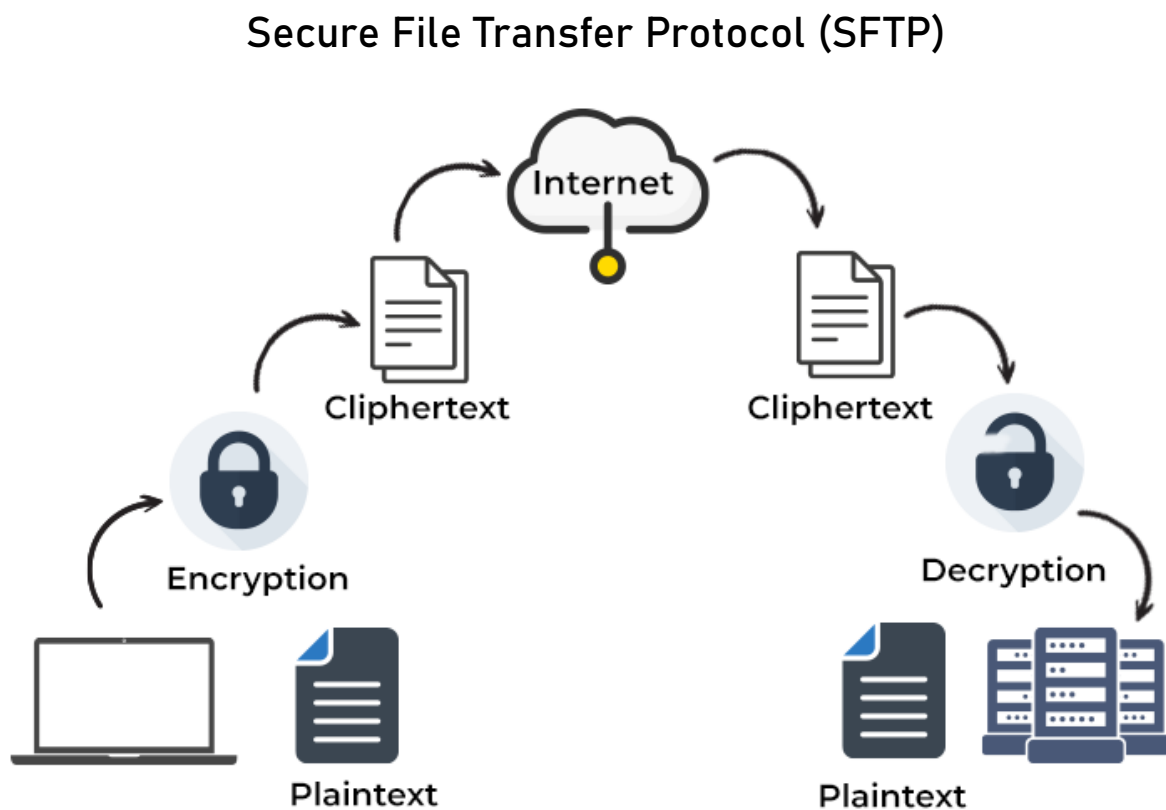
This diagram includes everything we have discussed so far including VPNs, Firewalls, and DMZ.



This updated design will protect the company from unauthorized access, cyberattacks, data theft, and other threats, ensuring the Confidentiality, Integrity and Availability (CIA) of data sent and received through the network.













c. Improvement of Internal FTP Server

To improve the security of the FTP, I would replace FTP with SFTP (Secure File Transfer Protocol).



SFTP is a secure version of FTP and is capable of transferring encrypted data using strong Encryption algorithms like shown in the picture above. It uses Secure Shell (SSH) for secure communication that ensures the confidentiality and integrity of the data.

(Singh, n.d.)

FTP vs. SFTP		
Features	FTP	SFTP
 <p>Strong Encryption Algorithms</p>		
 <p>Encrypts Usernames and Passwords</p>		
 <p>Key-based Authentication</p>		
 <p>Firewall Friendly</p>		

In addition to that, I'd also implement the following measures:

- Apply access control to restrict unauthorized access to the server.
- Keep the SFTP server software always up-to-date.
- A logging system to catch and fix any issues.
- Provide training to staff on how to manage and transfer sensitive files and document via the SFTP server.

Task 4 – Security Maintenance – 10 Marks

To maintain and monitor the effectiveness of the network's security, Wonder Telecoms should:

1. Regularly apply patches and updates to fix any newly found vulnerabilities.
2. Regularly review logs to identify any suspicious activities, unauthorized access attempts, and other security incidents.
3. Maintain an incident response plan and regularly test its effectiveness.
4. Conduct periodic security audits and assessments by third-party professionals.
5. Provide security training to employees.
6. Conduct regular risk assessments to identify new risks and assess the effectiveness of existing security controls.

7. Review and update security policies and procedures to meet industry best practices and requirements.
8. Keep softwares and devices up to date.

By maintaining these steps, Wonder Telecoms can ensure the effectiveness of their security strategies.

(Stallings, 2010)

Task 5 – Reflective Commentary – 10

Marks

During this assignment, I had no specific problems. However, some questions were not clear and structured properly. But I got an idea of what it was trying to ask somewhat and hopefully I answered them all correctly. When I got stuck in a question, I referred to the presentation on this unit by NCC.

Overall, I managed to complete this assignment without any major issues and tried my best to showcase my skills and knowledge I know about Network Security and Cryptography.

If I had to write this assignment again, I would try to provide more specific details, examples, diagrams and references to make my answers much better. Furthermore, I would try to keep my tone consistent throughout the report. I would also like to see if there could have been a different, a better and much more reliable approach to improve the network security of the company.

References

Barker, W., 2003. *Guideline for Identifying an Information System as a National Security System*. s.l.:National Institute of Standards and Technology.

NIST, 2016. *CVE-2016-8740 Detail*. s.l.:National Institute of Standards and Technology.

NIST, 2021. *CVE-2022-29929 Detail*. s.l.:National Institute of Standards and Technology.

NIST, 2023. *CVE-2023-25690 Detail*. s.l.:National Institute of Standards and Technology.

Scambray, J., McClure, S. & Kurtz, G., 2000. *Hacking Exposed: Network Security Secrets & Solutions*. 2nd ed. s.l.:McGraw-Hill.

Singh, A., n.d. *What is SFTP?*. [Online]
Available at: <https://www.educba.com/what-is-sftp/>

Stallings, W., 2010. *Cryptography and Network Security: Principles and Practice*. 5th ed. s.l.:Pearson.

Tanenbaum, A. S., 2002. *Computer Networks*. 4th ed. s.l.:Prentice Hall.

Thomas, S. A., 2000. *SSL & TLS Essentials: Securing the Web*. s.l.:Wiley.

Tracy, M., Jansen, W., Scarfone, K. & Butterfield, J., 2007. *Guidelines on Electronic Mail Security*. 2nd ed. s.l.:National Institute of Standards and Technology.

Zwicky, E. D., Cooper, S. & Chapman, D. B., 2000. *Building Internet Firewalls*. 2nd ed. s.l.:O'Reilly Media, Inc..