Student´s task sheet **TOPIC: Security**

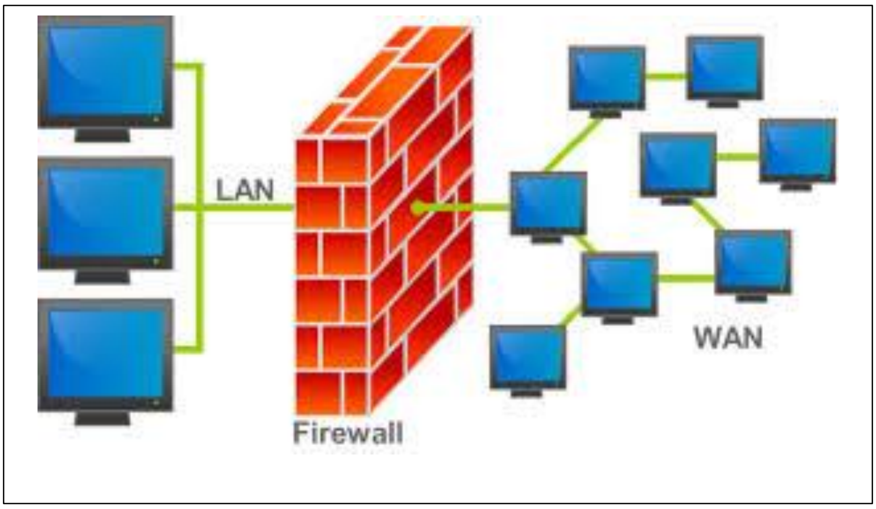
12

PART TWO	**Information Technology Technical Question**	**3 mins**

In this part of the exam, you will talk about **Security (firewall, VPN, encryption, antivirus protection)**. The following ideas will help you.

- Explain what **firewall, VPN, encryption, and antivirus protection** are.
- How can VPNs and encryption help protect privacy?
- Why is it important to have a secure network?
- Have you ever encountered a security threat on a computer network you were using? How did you respond?
- What's one thing you wish more people knew about protecting their data and privacy on computer networks?

2A



2B

McAfee
B
Bitdefender
norton
AVG
Malwarebytes

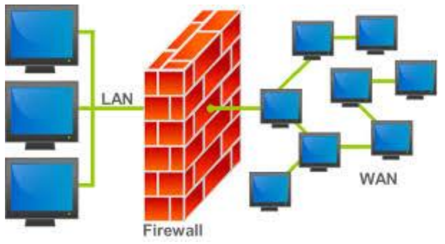
12

INTERLOCUTOR´S TASK SHEET **TOPIC: Security**

PART TWO **Information Technology Technical Question** **3 mins**

In this part of the exam, you will talk about Security (firewall, VPN, encryption, antivirus protection). The following ideas will help you.

- Explain what firewall, VPN, encryption, and antivirus protection are.
- How can VPNs and encryption help protect privacy?
  - **A firewall** is a security device that **monitors and controls** incoming and outgoing network traffic based on predetermined **security rules.** It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet. Firewalls can be hardware-based, software-based, or a combination of both.
  - **VPN (Virtual Private Network)** creates a **secure, encrypted connection** over a less secure network, such as the internet. It allows users to send and receive data as if their devices were directly connected to a private network. VPNs are commonly used to **protect sensitive data** and ensure **privacy** when accessing the internet from remote locations.
  - **Encryption** is the process of converting data into a **coded format to prevent unauthorized access**. Only authorized parties with the correct decryption key can access the original data. Encryption is used to protect data in transit (e.g., during online transactions) and data at rest (e.g., stored on a hard drive).
  - **Antivirus Protection: Antivirus software** is designed **to detect, prevent**, and **remove malicious software** (malware) such as viruses, worms, and trojans. It scans files and programs for known threats and monitors system behaviour for suspicious activity. Regular updates are essential to keep antivirus software effective against new threats.
- Why is it important to have a secure network?
- Have you ever encountered a security threat on a computer network you were using? How did you respond?
- What's one thing you wish more people knew about protecting their data and privacy on computer networks?



2A

2B