**5.1 Lesson: Network Security Fundamentals (Firewalls, IDS/IPS, VPNs)**

Network Security Fundamentals encompass critical components designed to protect networks from unauthorized access, misuse, or damage. The primary elements include Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Virtual Private Networks (VPNs).

Firewalls serve as a barrier between internal networks and external sources that may pose threats. They monitor incoming and outgoing traffic and enforce predetermined security rules to prevent unauthorised access.

Intrusion Detection Systems (IDS) are essential for monitoring network traffic for signs of suspicious activity or policy violations. By analysing data packets against known threat signatures, IDS can alert administrators to potential breaches or anomalies.

Intrusion Prevention Systems (IPS) build on the functions of IDS by taking proactive steps to block detected threats in real time. This capability is vital for minimising the impact of cyber-attacks on an organisation's infrastructure.

Virtual Private Networks (VPNs) provide secure connections over the internet by encrypting data transmitted between users and their target networks. This encryption protects sensitive information from interception while enabling users to maintain privacy and anonymity online.

Collectively, these components form a robust framework of network security that helps safeguard organizational assets against escalating cyber threats.