A firewall is a network security system designed to monitor and control incoming and outgoing network traffic based on predetermined security rules.They are capable of blocking sophisticated threats, such as malware and advanced persistent threats (APTs), and are more effective at managing network traffic in modern environments.Next-Generation Firewalls (NGFW): NGFWs combine traditional firewall functionality with advanced features like deep packet inspection, intrusion prevention systems (IPS), and application-level filtering.Preventing Cyberattacks: Firewalls can block traffic associated with common cyberattacks like Distributed Denial of Service (DDoS) attacks, port scanning, or attempts to exploit known software vulnerabilities.Advanced firewalls (Next-Generation Firewalls) include features like intrusion detection/prevention systems (IDS/IPS), antivirus, and anti-malware capabilities.Types of Firewalls: Packet-Filtering Firewalls: These are the simplest type of firewall, filtering traffic based on predefined rules about IP addresses, port numbers, and protocols.It acts as a barrier between a trusted internal network (like a company's private network) and untrusted external networks (such as the internet), filtering out malicious traffic and preventing unauthorized access.Blocking Unwanted Traffic: Firewalls help block unsolicited and potentially harmful traffic from the internet or other external sources.Network Segmentation: Firewalls can create different zones within a network, such as separating internal networks from external-facing services (e.g., web servers, email servers).Proxy Firewalls: Proxy firewalls act as intermediaries between the user and the network, making requests on behalf of the user and filtering content based on predefined security rules.Protocols: Controlling traffic based on the communication protocol being used (e.g., HTTP, FTP, DNS).These logs are essential for .identifying vulnerabilities, troubleshooting issues, and auditing network traffic