ZIAUDDIN UNIVERSITY

QUIZ NO: 2

COURSE: COMPUTER COMMUNCATIONS & NETWORKS

SUBMITTED TO: SIR NAUMAN

STUDENT: MIRZA ABDULLAH BAIG (004)

FIELD: DATA SCIENCE

Q: Define Firewall and Network Security.

Ans: Firewall:

A firewall is a type of cyber security tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons. The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through. Firewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewalls:

- Packet-filtering firewalls
- Circuit-level gateways
- Stateful inspection firewalls
- Application-level gateways (a.k.a. proxy firewalls)
- Next-gen firewalls
- Software firewalls
- Hardware firewalls
- Cloud firewalls

Network Security:

Network security is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today. A well designed network security solution reduces overhead expenses and safeguards organizations from costly losses that occur from a data breach or other security incident. Ensuring legitimate access to systems, applications and data enables business operations and delivery of services and products to customers.