SNS COLLEGE OF TECHNOLOGY

Coimbatore-35

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade

Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

19ECT301- COMMUNICATION NETWORKS

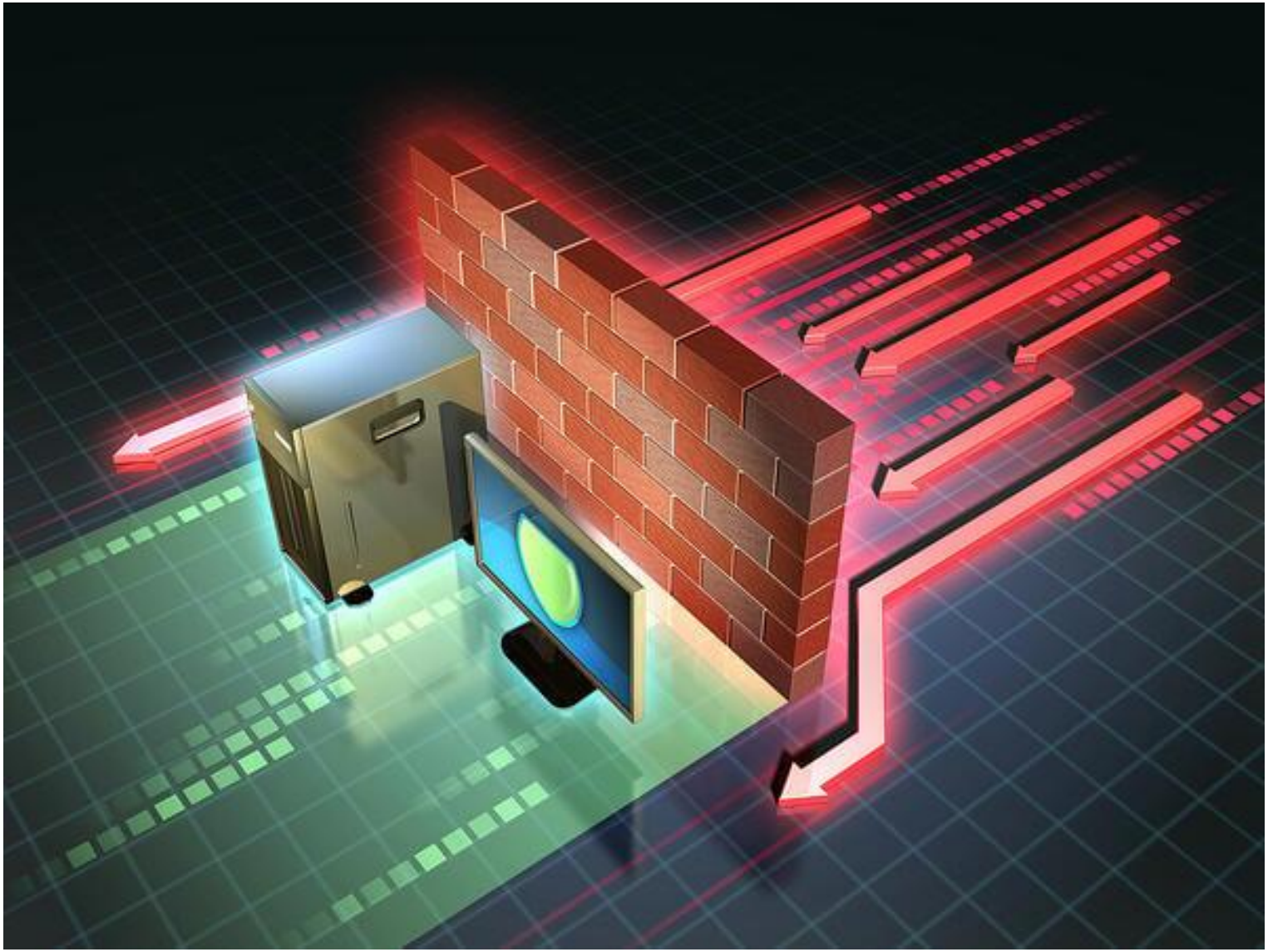
III YEAR/ V SEMESTER

UNIT 4 –NETWORK & DATA SECURITY

TOPIC 6 – FIREWALLS – TYPES COMPARISON OF FIREWALL TYPES

- A firewall is a type of cybersecurity tool used to filter traffic on a network. Firewalls can 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 unique pros and cons.



Firewall Types:

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

Firewall Delivery Methods:

- Software firewalls
- Hardware firewalls
- Cloud firewalls

Type 1: Packet-Filtering Firewalls

As the most “basic” and oldest type of firewall architecture, packet-filtering firewalls create a checkpoint at a traffic router or switch. The firewall performs a simple check of the data packets coming through the router—inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level details without opening the packet to examine its contents. It then drops the packet if the information packet doesn’t pass the inspection.

The good thing about these firewalls is that they aren’t very resource-intensive. Using fewer resources means they are relatively simple and don’t significantly impact system performance. However, they’re also relatively easy to bypass compared to firewalls with more robust inspection capabilities.

Type 2: Circuit-Level Gateways

Circuit-level gateways are another simplistic firewall type meant to quickly and easily approve or deny traffic without consuming significant computing resources. Circuit-level gateways work by verifying the transmission control protocol (TCP) handshake. This TCP handshake check is designed to ensure that the session the packet is from is legitimate.

While extremely resource-efficient, these firewalls do not check the packet itself. So, if a packet held malware but had the proper TCP handshake, it would easily pass through. Vulnerabilities like this are why circuit-level gateways are not enough to protect your business by themselves.