SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

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 AND COMMUNICATION ENGINEERING

COURSE NAME : 19EC625 – CYBER FORENSIC AND DATA SECURITY

III YEAR / VI SEMESTER

Unit II- E-MAIL SECURITY & FIREWALLS

Topic : Terminologies in Firewall

What is a Firewall?

➢ Definition

A firewall is a network security system. It monitors and controls incoming and outgoing traffic.

➢ Purpose

Firewalls prevent unauthorized access. They protect networks from cyber threats.

➢ Function

They act as a barrier between trusted and untrusted networks. This is essential for maintaining security.

Packet Filtering

Examination

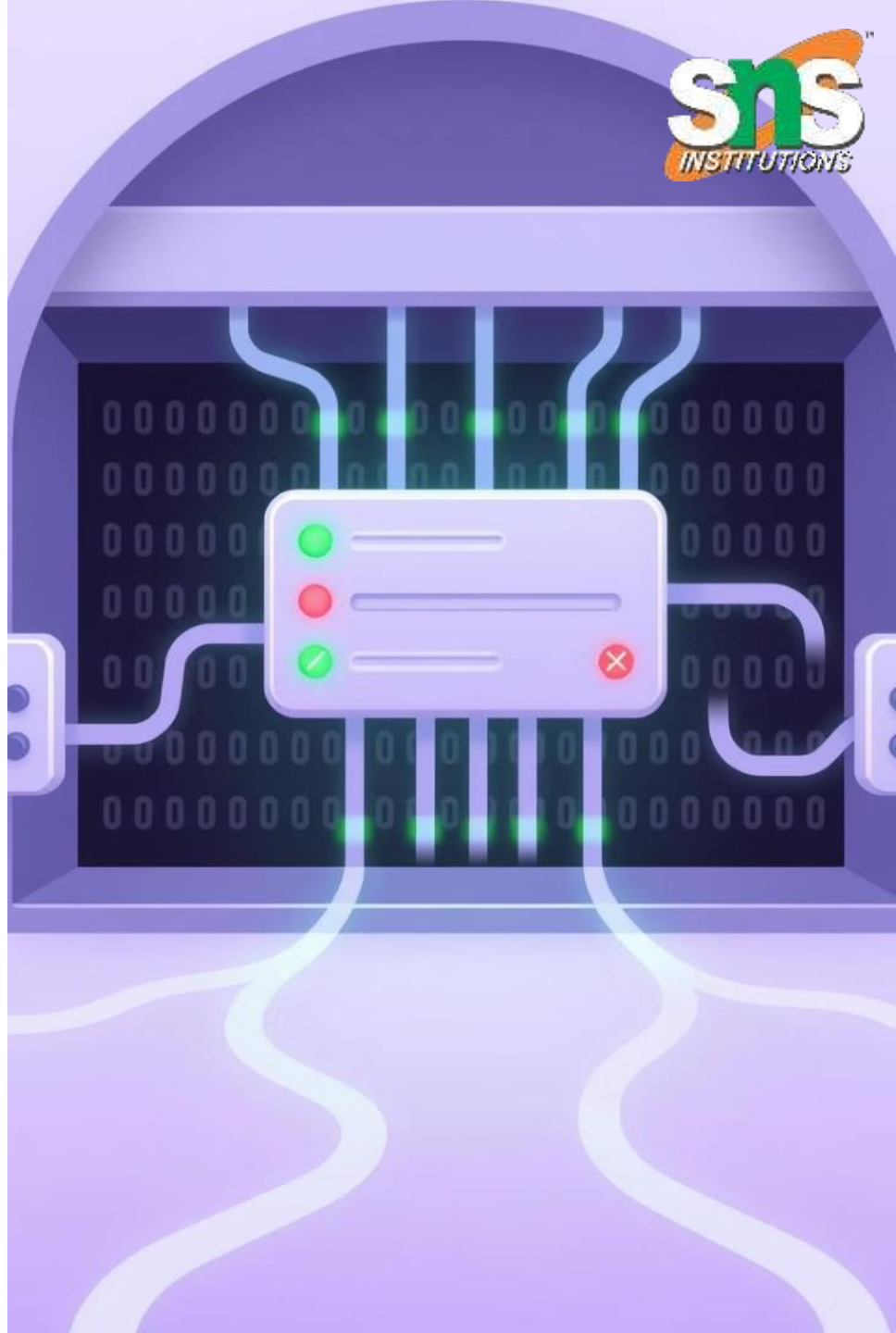
Packet filtering examines individual packets. It analyzes header information.

Rules

Firewalls use predefined rules. They determine whether to allow or deny packets.

Criteria

Common criteria include source, destination, and port. These help filter effectively.



Stateful Inspection

Connection Tracking

Tracks the state of network connections.

State Table

Maintains a record of active connections.

Enhanced Security

Offers a more secure approach than packet filtering.

Virtual Private Networks (VPNs)

1. Secure Connection
2. Remote Access
3. Encryption

VPNs create secure, encrypted connections. They allow remote users to access networks securely. VPNs ensure data privacy and security.

IDS/IPS

Threat Detection

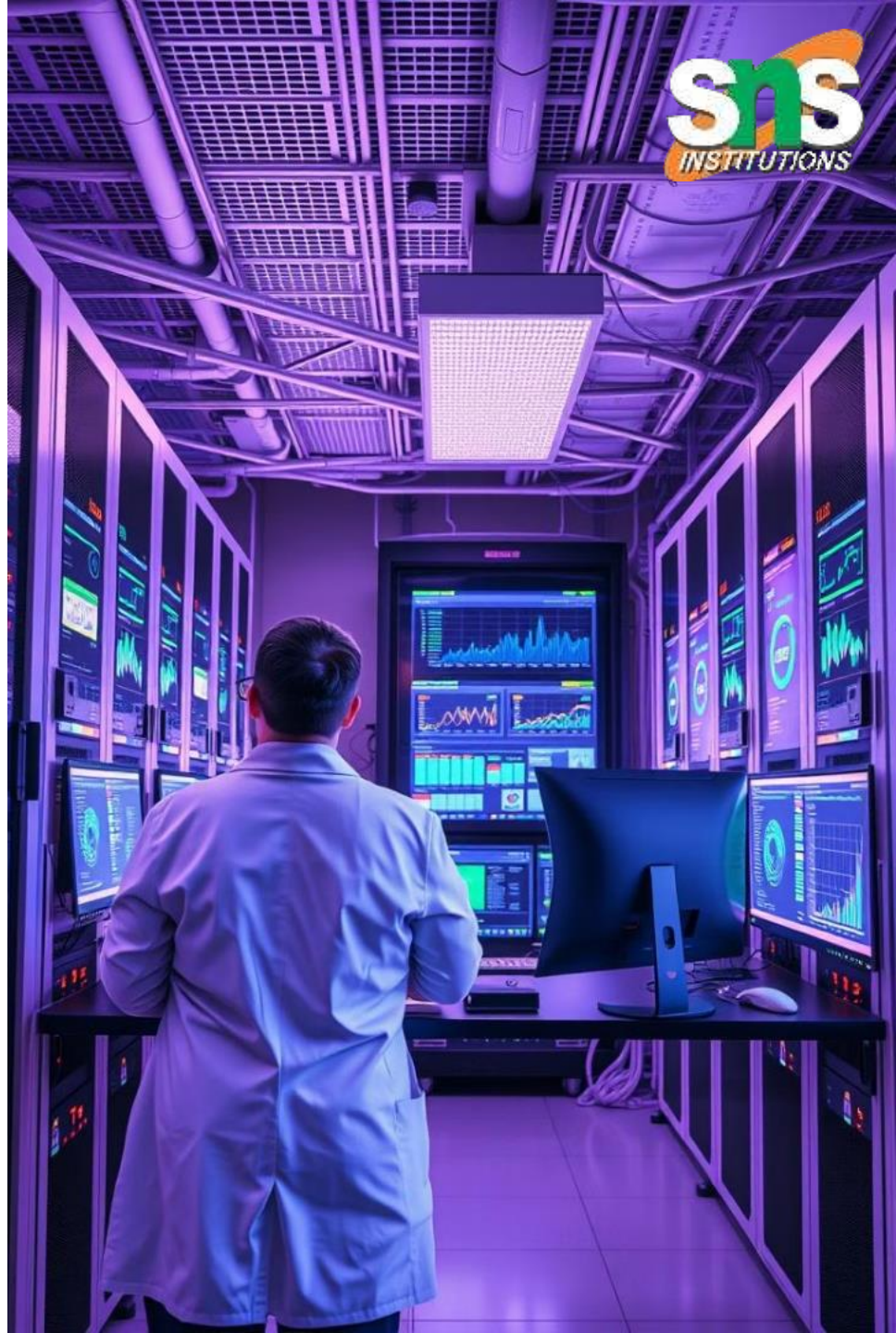
Intrusion Detection Systems detect malicious activity.

Threat Prevention

Intrusion Prevention Systems prevent threats in real time.

Security

Both systems enhance network security and threat response.



Next-Generation Firewalls (NGFWs)

1 **Advanced Features**

NGFWs offer advanced features. These include deep packet inspection.

2 **Application Control**

Application control enables granular policies. This manages application usage.

3 **Threat Intelligence**

Integrated threat intelligence enhances detection. This prevents sophisticated attacks.

Common Firewall Rules

80

HTTP

Allow web traffic on port 80.

443

HTTPS

Enable secure web traffic on 443.

22

SSH

Secure Shell access is enabled via 22.

25

SMTP

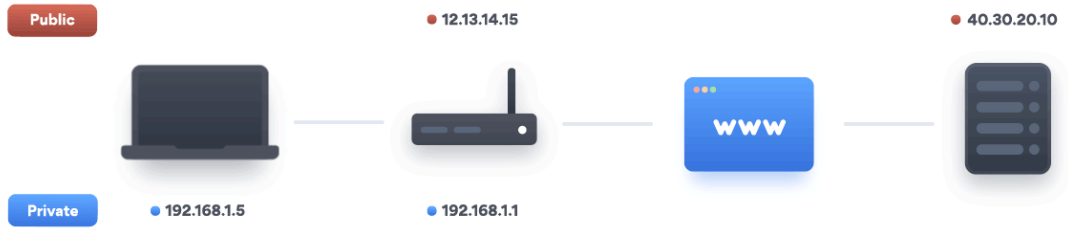
Allow email traffic on port 25.

Deep Packet Inspection (DPI)

1	Packet Content
2	Malware
3	Intrusion

Deep packet inspection analyzes the content of network packets. It detects malware and intrusions. DPI provides more in-depth security.

NAT



NAT (Network Address Translation)

Definition:

NAT translates private IP addresses within a local network to a single public IP address, allowing multiple devices to share one public IP.

Key Benefits:

IP Address Conservation: Reduces the need for multiple public IP addresses.

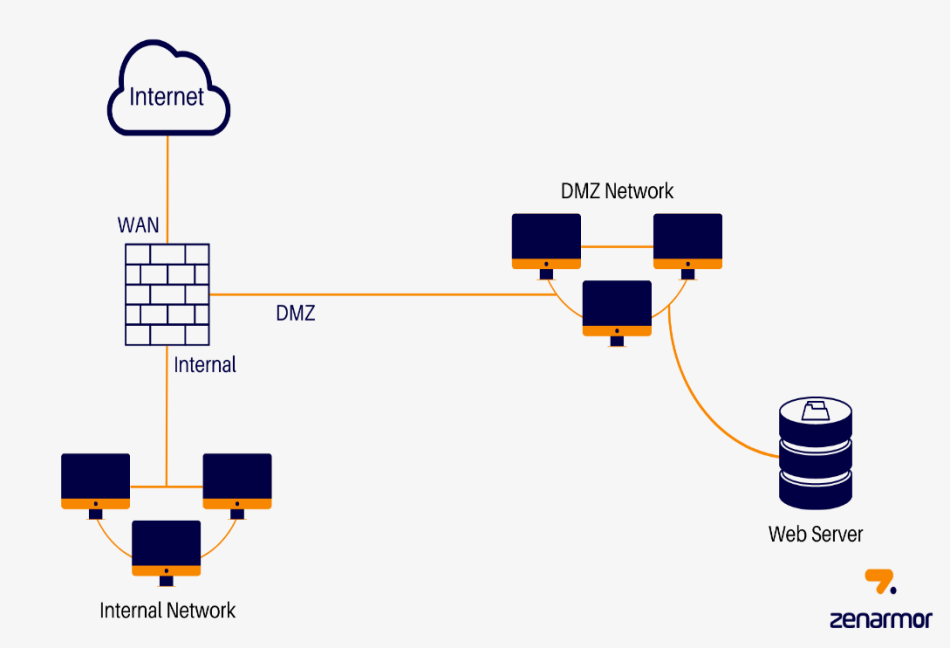
Security: Hides internal IP addresses from external networks, adding an extra layer of security.

Flexibility: Allows internal devices to communicate with external networks seamlessly.

DMZ

DMZ (Demilitarized Zone)

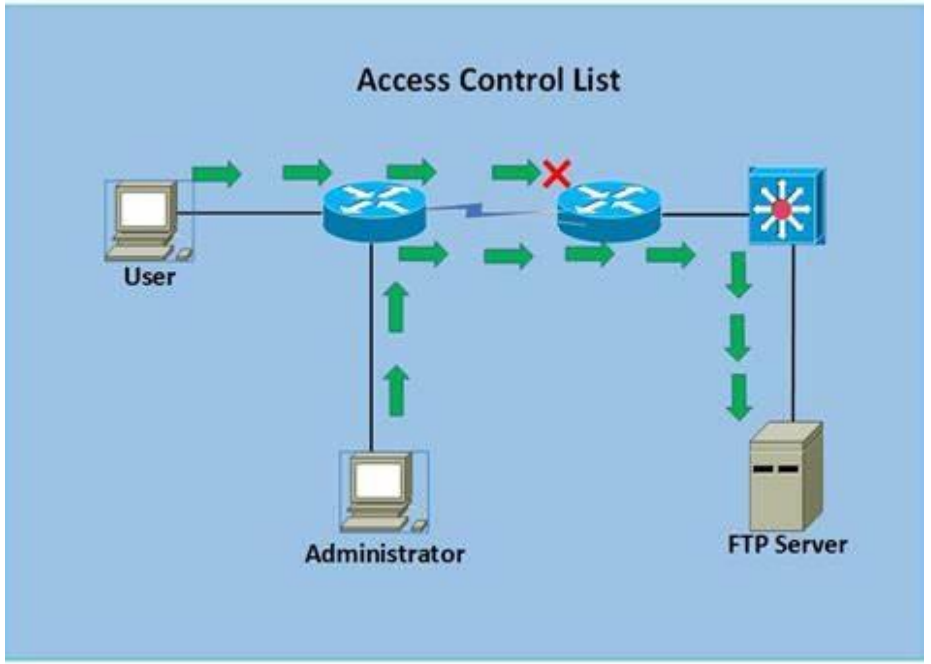
- **Definition**:
  - A DMZ is a separate network that acts as a buffer zone between the internal network and the public internet, adding an extra layer of security.
- **Purpose**:
  - To provide a secure environment for internet-facing services while protecting the internal network from potential threats.



ACL

Access Control List (ACL)

- **Definition**:
  - An ACL is a list of permissions attached to an object that specifies which users or systems can access the object and what operations they can perform.
- **Purpose**:
  - To provide granular control over who can access specific resources and what actions they can take.



Conclusion

- Understanding firewall terminologies is vital for robust network security.
- Packet filtering, stateful inspection, and proxy servers are key. NAT, DPI, VPNs, and IDS/IPS are also important.
- Proper implementation enhances threat protection.