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 COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit III- Network Threats

Topic : Threats to Server security.

Threats to Server security

Servers are **essential components of network infrastructure**, and their security is critical for ensuring the confidentiality, integrity, and availability of data.

There are common threats to server security in networking:

1.Malware and viruses:

- Malware and viruses can infect servers and compromise their security.
- Malware can be introduced to a server through email attachments, downloads, or infected devices. Once installed, malware can steal data, cause system disruptions, or provide unauthorized access to the server.

2.Denial of Service (DoS) attacks:

- DoS attacks involve overwhelming a server with traffic to the point that it becomes unavailable to legitimate users.
- DoS attacks can be launched using a variety of techniques, including flooding the server with traffic or exploiting vulnerabilities in the server's operating system or applications.

3.Unauthorized access:

- Unauthorized access to a server can occur when an attacker gains access to the server through weak passwords, vulnerabilities in software, or other means.
- Once an attacker gains access, they can steal sensitive data, manipulate or delete files, or use the server for malicious purposes.

4.Insider threats:

- Insider threats to server security can come from employees, contractors, or other insiders who have authorized access to the server.
- These threats can include intentional actions, such as stealing data or damaging the server, or unintentional actions, such as accidentally deleting important files.

5.Physical threats:

- Physical threats to server security can include theft, vandalism, or damage caused by natural disasters or accidents.
- Physical security measures, such as access controls and surveillance cameras, can help prevent these types of threats.

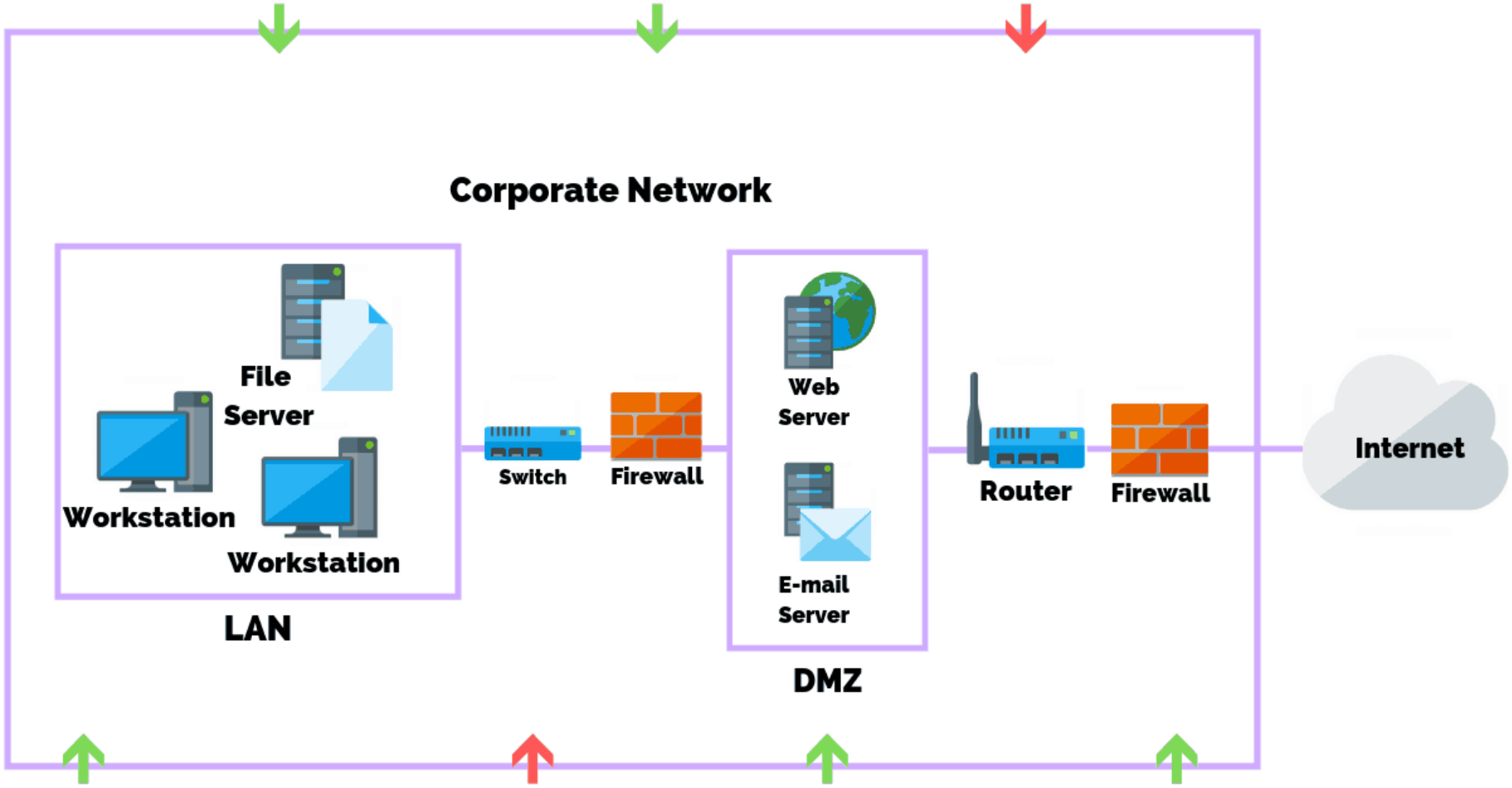
To prevent these threats,

- organizations should **implement strong access controls**, use up-to-date antivirus software, and perform regular vulnerability scans and patches.
- It is also important to **monitor server activity for suspicious behavior** and conduct regular security audits to identify and address any weaknesses in the server's security.
- Additionally, organizations should have a **plan in place for incident response and disaster recovery to minimize** the impact of any security incidents.

- A network has two components – hardware and software.
- Both these components have their own vulnerability to threats.
- **Threat** is a possible risk that might exploit a network weakness to breach security and cause harm. Examples of hardware threats include –

- Improper installation
- Use of unsecure components
- Electromagnetic interference from external sources

- Extreme weather conditions
- Lack of disaster planning
- Hardware threats form only 10% of network security threats worldwide because the components need to be accessed physically.
- 90% threats are through software vulnerabilities. Here we discuss the major types of software security threats.


Corporate Network
File
Server
Workstation
Workstation
LAN
Switch
Firewall
Web
Server
E-mail
Server
DMZ
Router
Firewall
Internet

Any Query????

Thank you……