Information Security
CS 3002

Dr. Haroon Mahmood

Assistant Professor

NUCES Lahore

Disaster Recovery Plan

- Provide guidance in the event of a disaster
- Clear establishment of priorities
- Clear delegation of roles & responsibilities
- Alert key personnel
- Document disaster
- Mitigate impact
- Evacuation of physical assets

Business Continuity Planning

- **The overall goal of BCP is to provide a quick, calm, and efficient response in the event of an emergency and to enhance a company's ability to recover from a disruptive event promptly.**

The BCP process has four main steps:

- **Project scope and planning**
- **Business impact assessment**
- **Continuity planning**
- **Approval and implementation**

Design of Security Architecture

- **Defenses in Depth,**
  - **Implementation of security in layers, policy, training, technology.**
  - **Requires that organization establish sufficient security controls and safeguards so that an intruder faces multiple layers of controls**

- **Security Perimeter**
  - **Point at which an organization's security protection ends and outside world begins**
  - **Does not apply to internal attacks from employee threats or on-site physical threats**

Key Technology Components

- **Firewall**
  - Device that selectively discriminates against information flowing in and out
  - Specially configured computer
  - Usually on parameter part of or just behind gateway router

- **Proxy Server**
  - Performs actions on behalf of another system
  - Configured to look like a web server
  - Assigned the domain name
  - Retrieves and transmits data
  - Cache server

Key Technology Components

- DMZ
  - Buffer against outside attacks
  - No mans land between computer and world
  - Web servers often go here
- IDS
  - Intrusion Detection System
    - Host based
      - Installed on machines they protect
      - Monitor host machines
    - Network based
      - Look at patterns of network traffic
      - Attempt to detect unusual activity
      - Requires database of previous activity
      - Uses “machine learning” techniques
      - Can use information form similar networks

Security Architecture

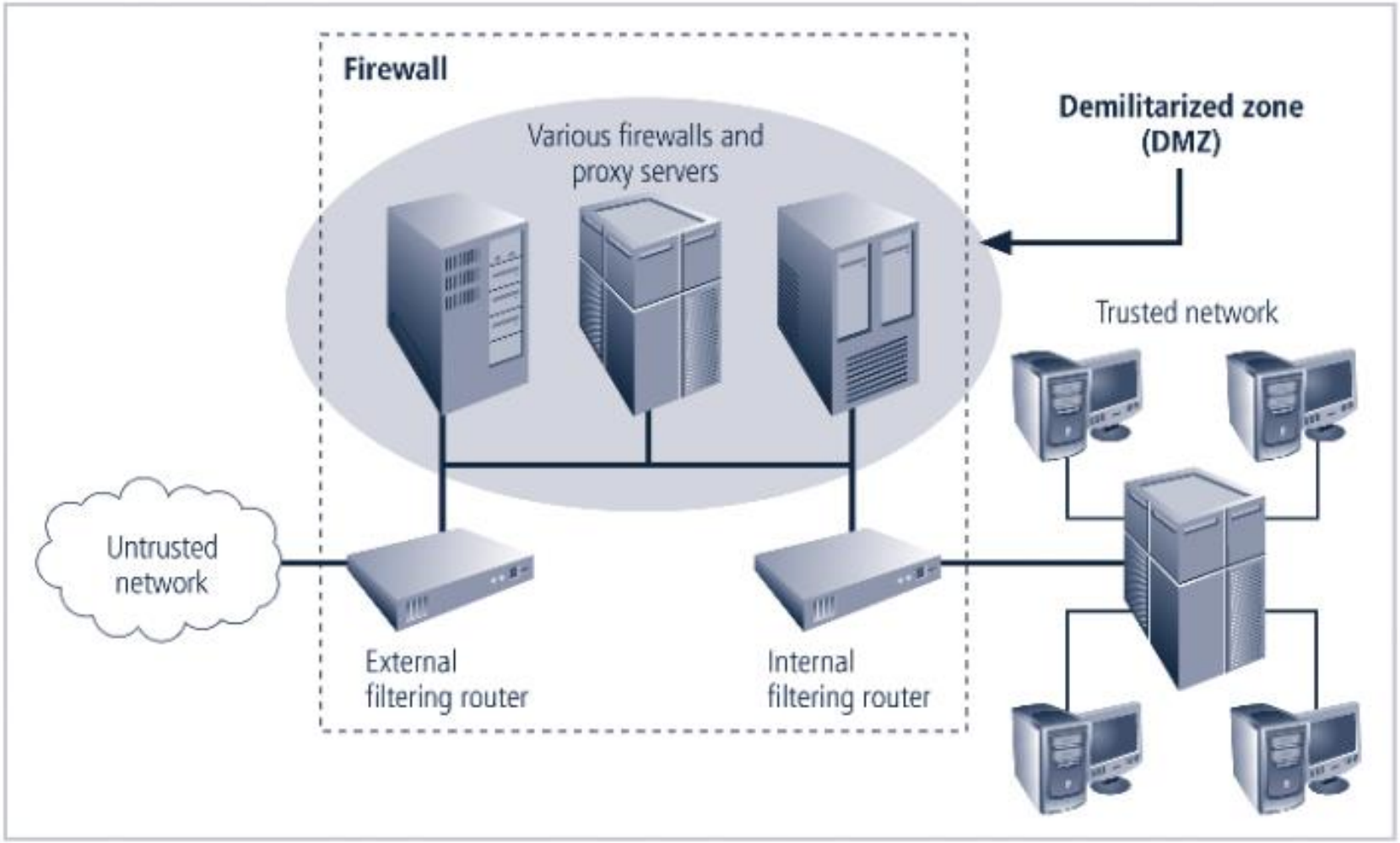

FIGURE 5-18 Firewalls, Proxy Servers, and DMZs

What is a malware?

- **“A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim.” (NIST – 2005)**
- **It is also called digital pest.**

What can it do?

- Steal personal information
- Delete files
- Make you click fraud
- Steal software serial numbers
- Use your computer as relay (Zombie)
- Corrupt files
- etc...