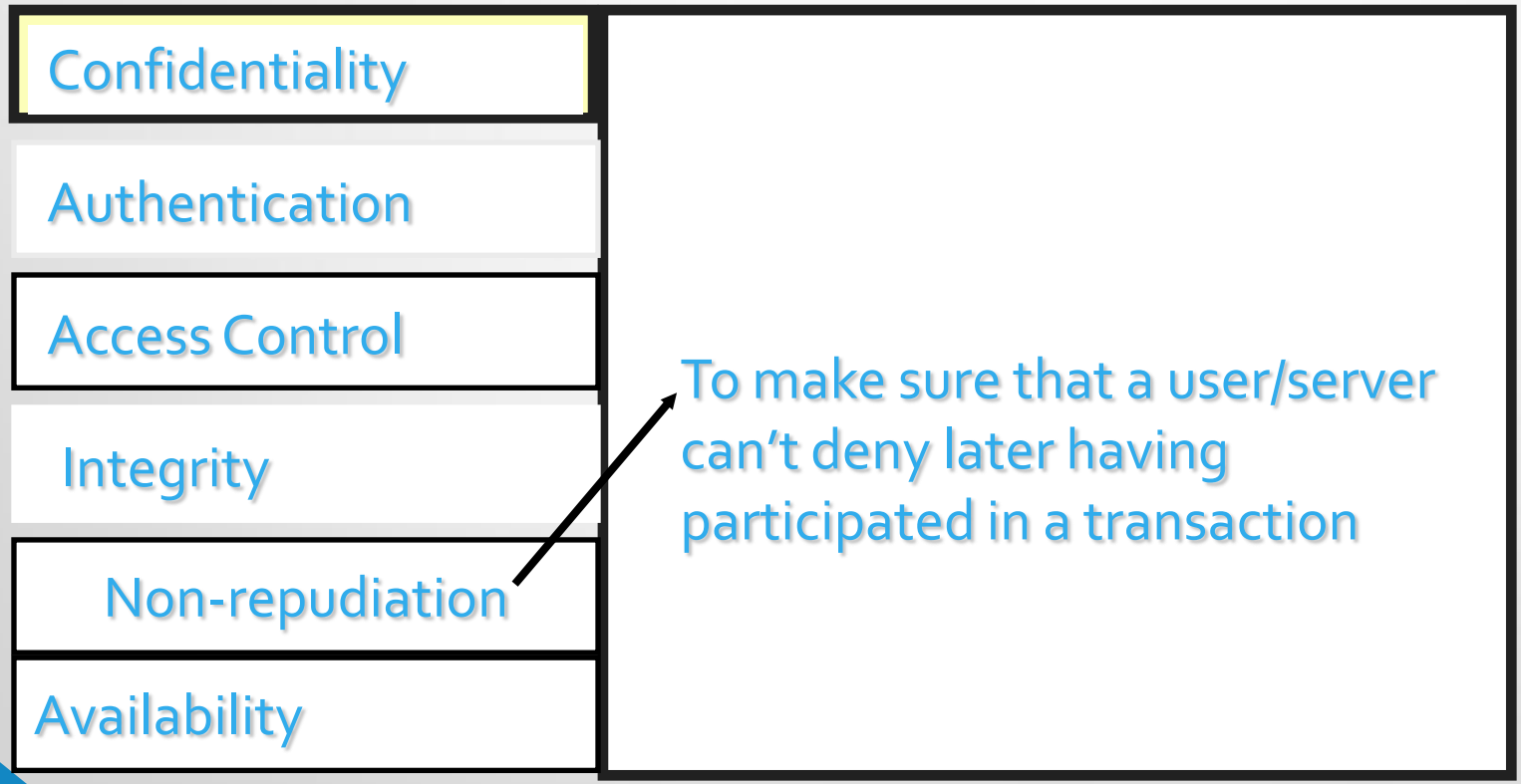
Information Security System
EC-615-F
Dronacharya College of Engineering

Lecture No 2

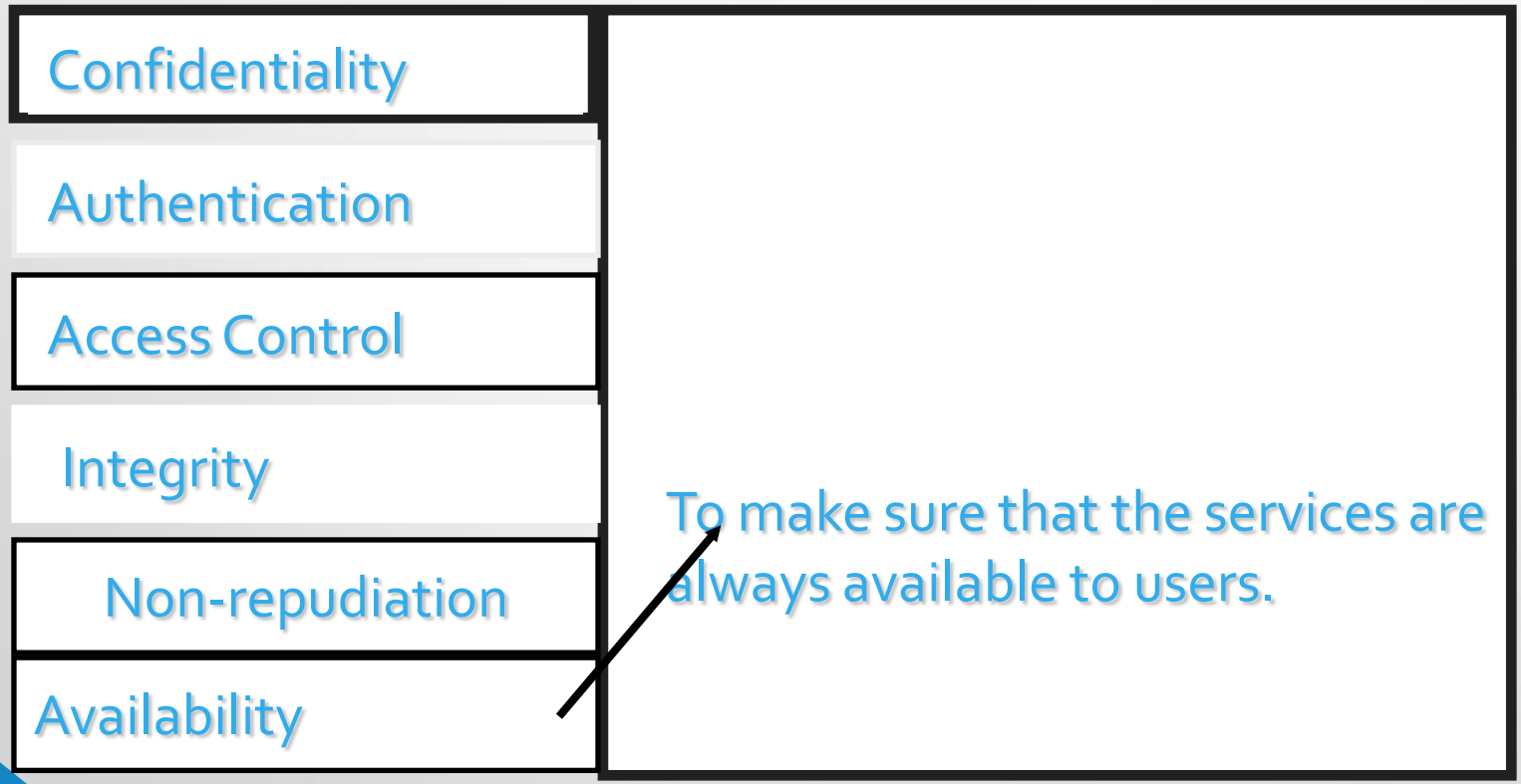
Topics covered

- **OSI security Architecture**
- **Security Architecture for WLAN**

Security Services: Non-repudiation



Security Services: Availability



Security Overview

- Introduction
- Security Services
- Overview of Existing Security Systems

Overview of Existing Security Systems : Firewalls

Used even for Deterring (Scaring attackers)

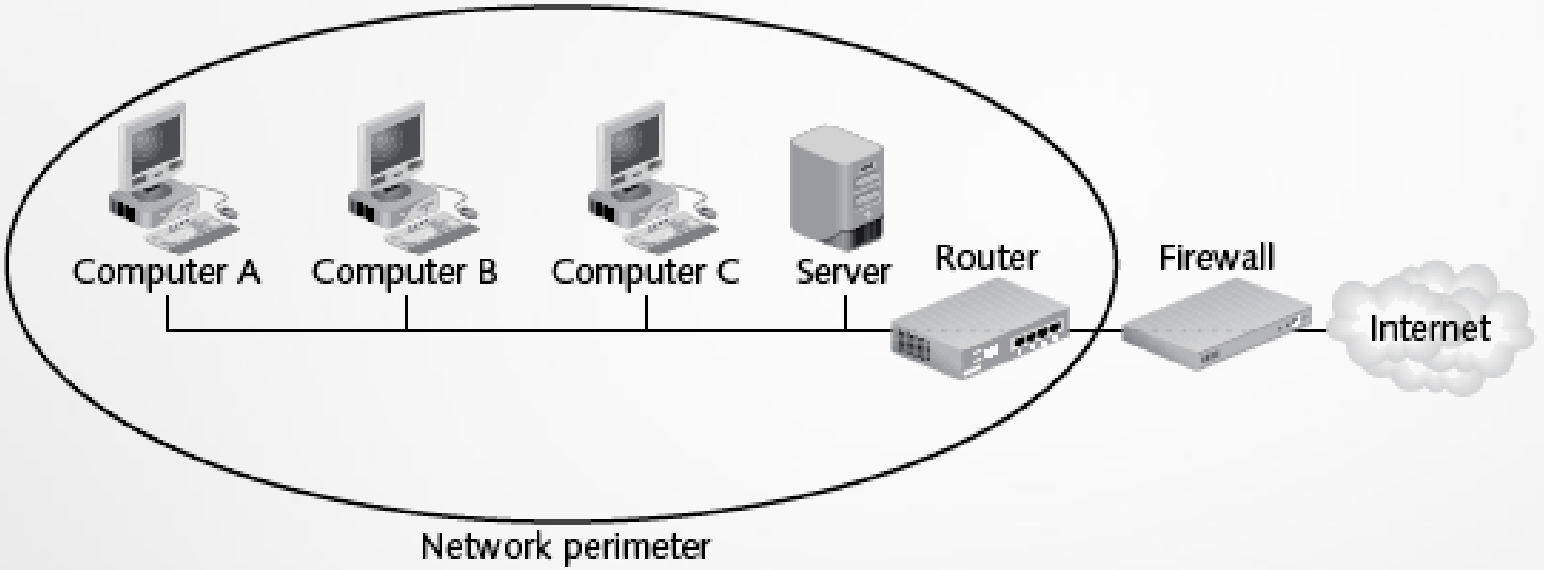


Figure 5-11 Firewall position in network

Firewalls → Designed to prevent malicious packets from entering

- Software based → Runs as a local program to protect one computer (personal firewall) or as a program on a separate computer (network firewall) to protect the network
- Hardware based → separate devices that protect the entire network (network firewalls)

Overview of Existing Security Systems : Detection -Intrusion Detection Systems

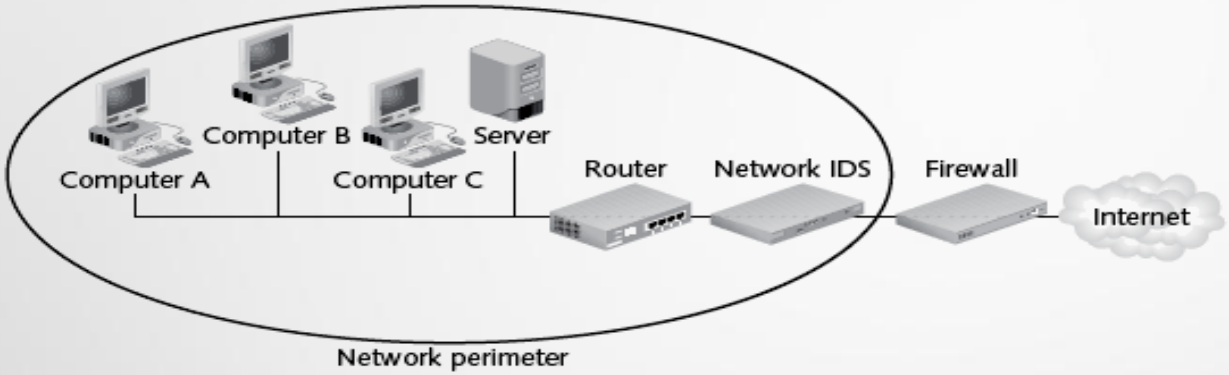


Figure 5-12 IDS system

Intrusion Detection System (IDS) → Examines the activity on a network

Goal is to detect intrusions and take action

Two types of IDS:

Host-based IDS → Installed on a server or other computers (sometimes all)

Monitors traffic to and from that particular computer

Network-based IDS → Located behind the firewall and monitors all network traffic

Overview of Existing Security Systems : Network Address Translation (NAT)

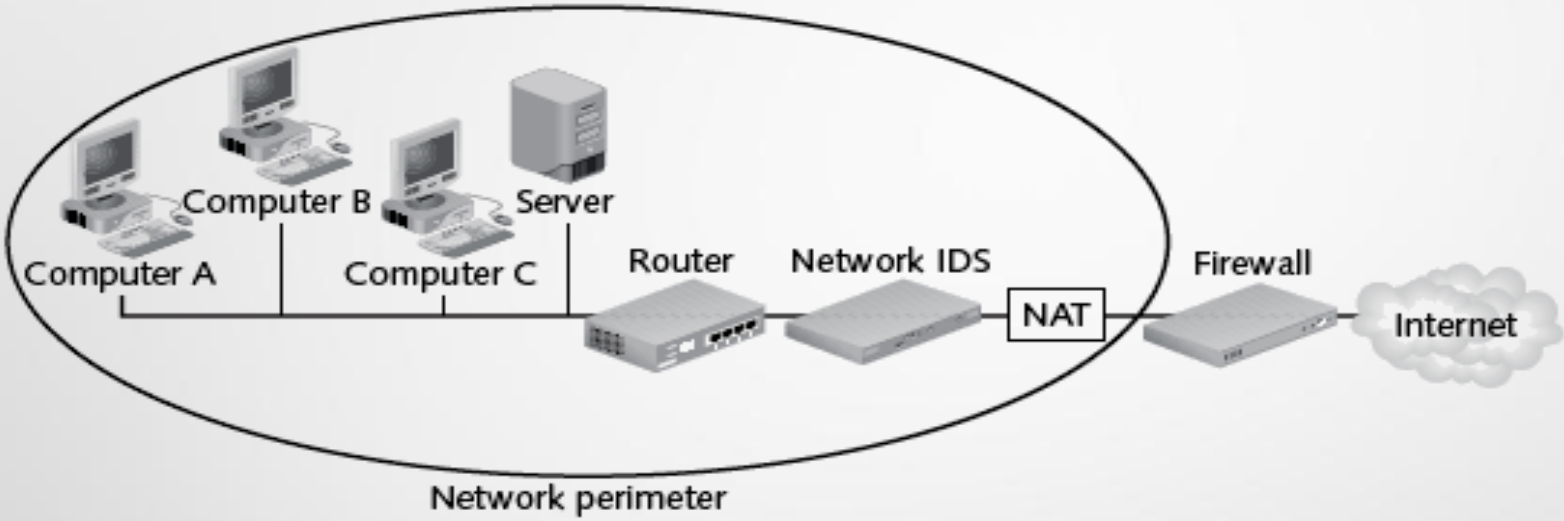


Figure 5-13 Network address translation position

Network Address Translation (NAT) Systems → Hides the IP address of network devices Located just behind the firewall. NAT device uses an alias IP address in place of the sending machine's real one "You cannot attack what you can't see"

Overview of Existing Security Systems : Proxy Servers

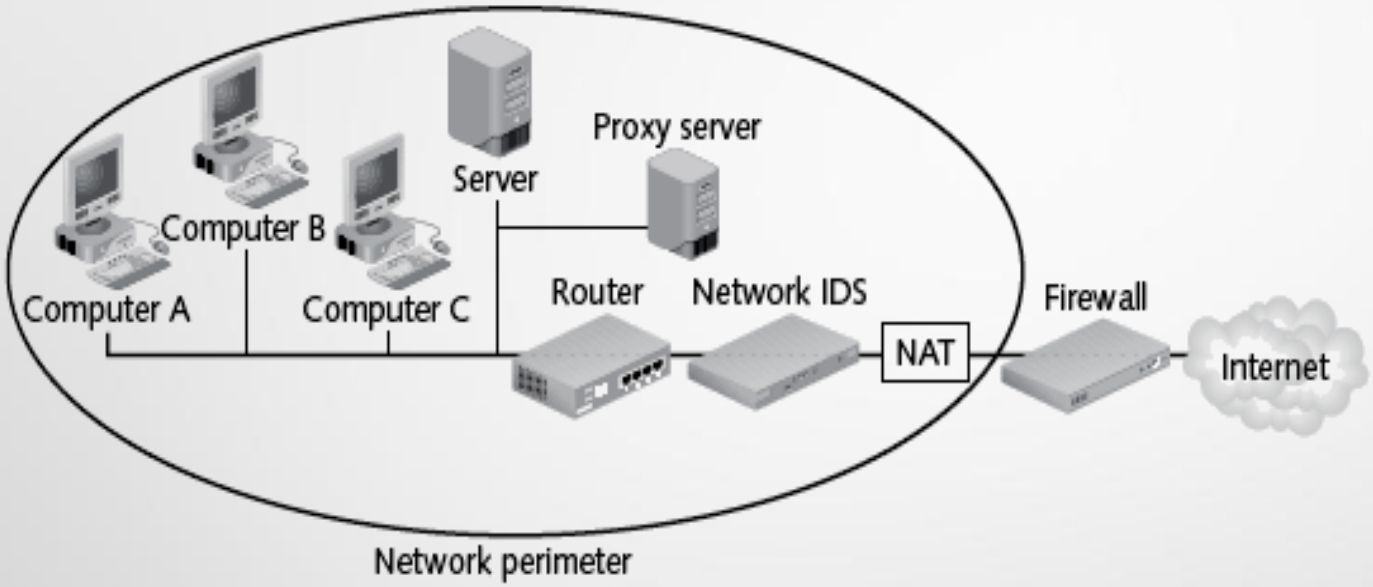


Figure 5-15 Proxy server location

Proxy Server → Operates similar to NAT, but also examines packets to look for malicious content
Replaces the protected computer's IP address with the proxy server's address
Protected computers never have a direct connection outside the networkThe proxy server intercepts requests. Acts "on behalf of" the requesting client

Adding a Special Network called Demilitarized Zone (DMZ)

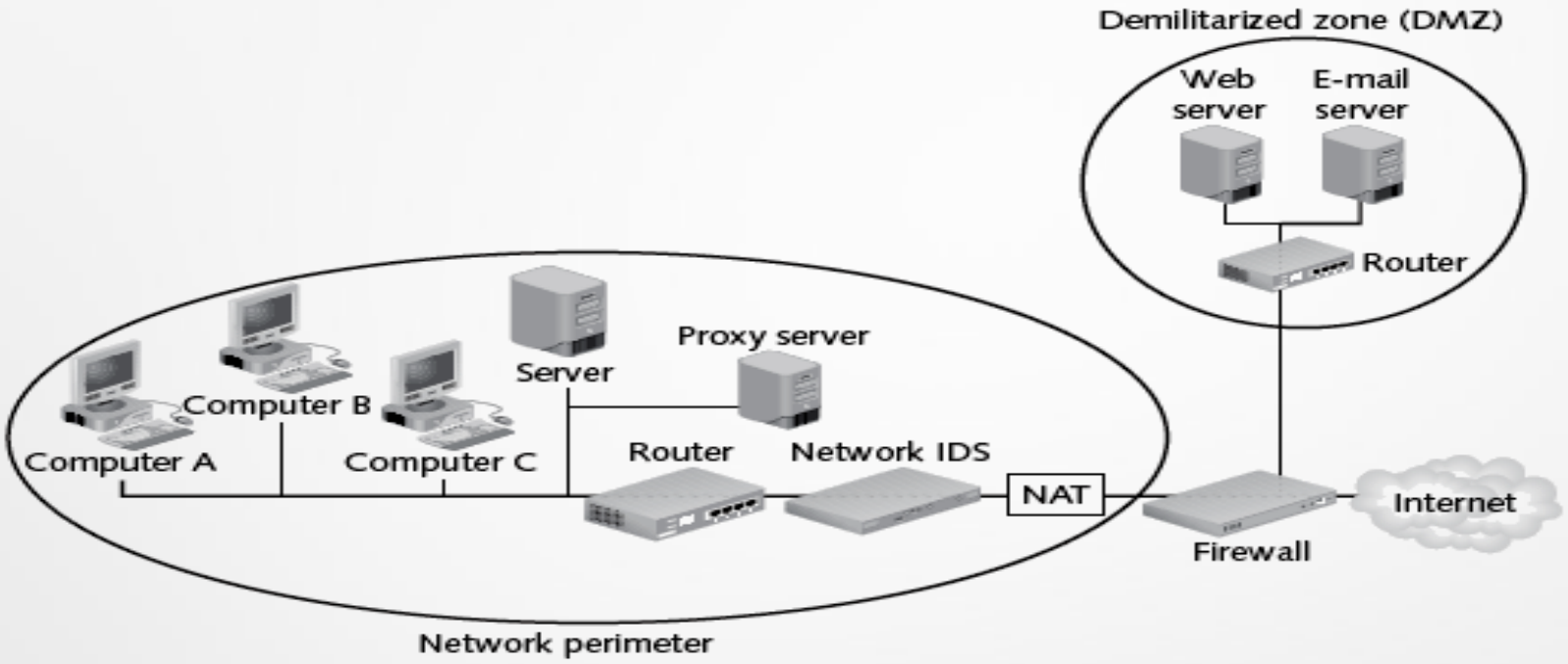


Figure 5-17 DMZ set up outside the secure network perimeter

- Demilitarized Zones (DMZ) → Another network that sits outside the secure network perimeter. Outside users can access the DMZ, but not the secure network
  - Some DMZs use two firewalls. This prevents outside users from even accessing the internal firewall → Provides an additional layer of security

Overview of Existing Security Systems : Virtual Private Networks (VPN)

- **Virtual Private Networks (VPNs)** → A secure network connection over a public network
  - **Allows mobile users to securely access information**
  - **Sets up a unique connection called a tunnel**

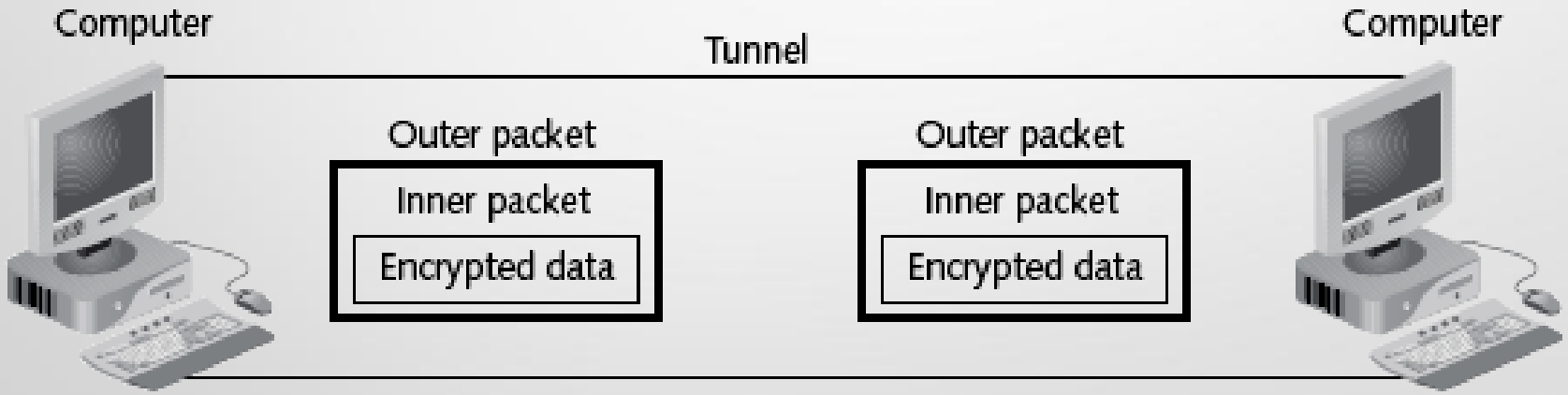


Figure 5-20 VPN transmission

Overview of Existing Security Systems : Virtual Private Networks (VPN)

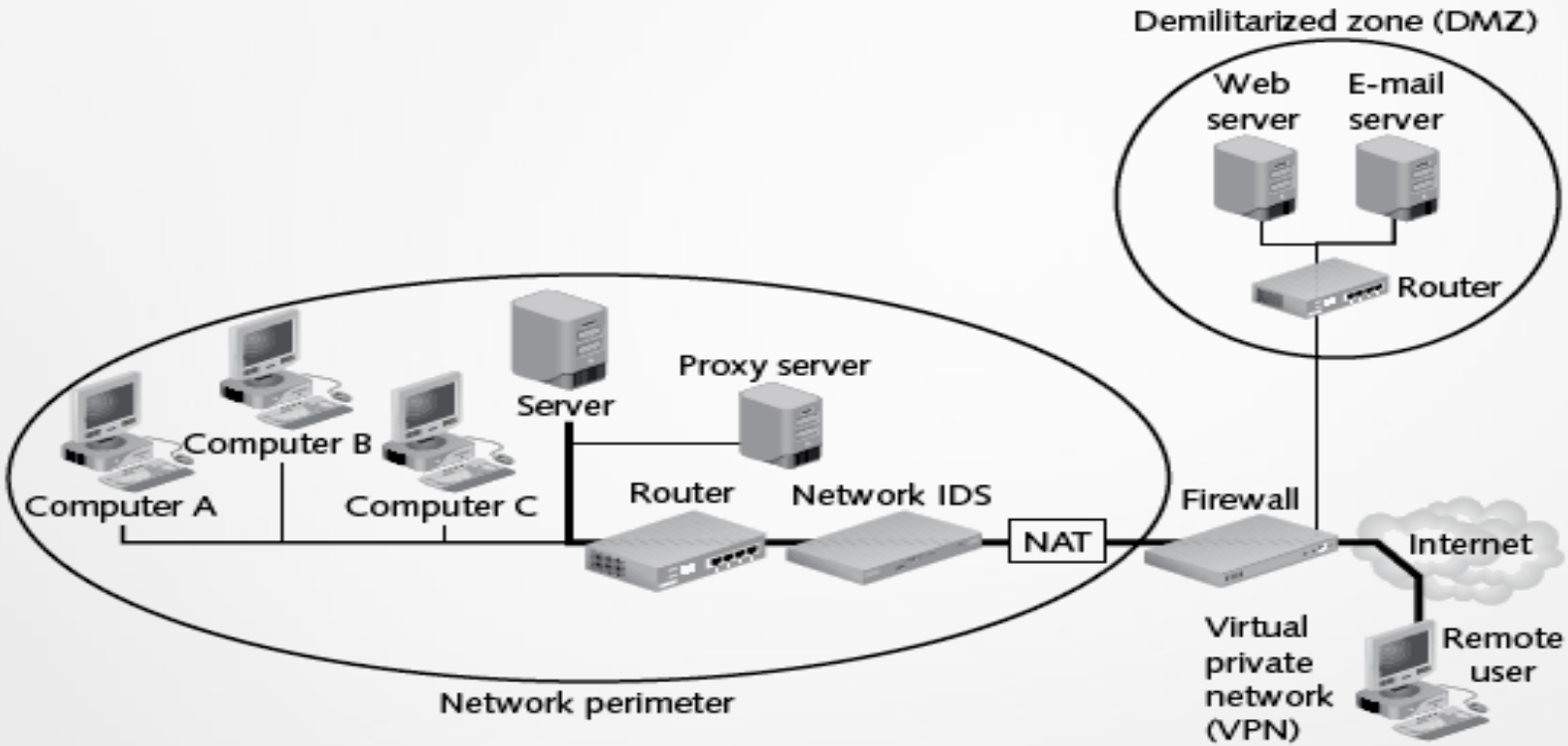


Figure 5-19 Virtual private network (VPN)

Overview of Existing Security Systems : Honeypots

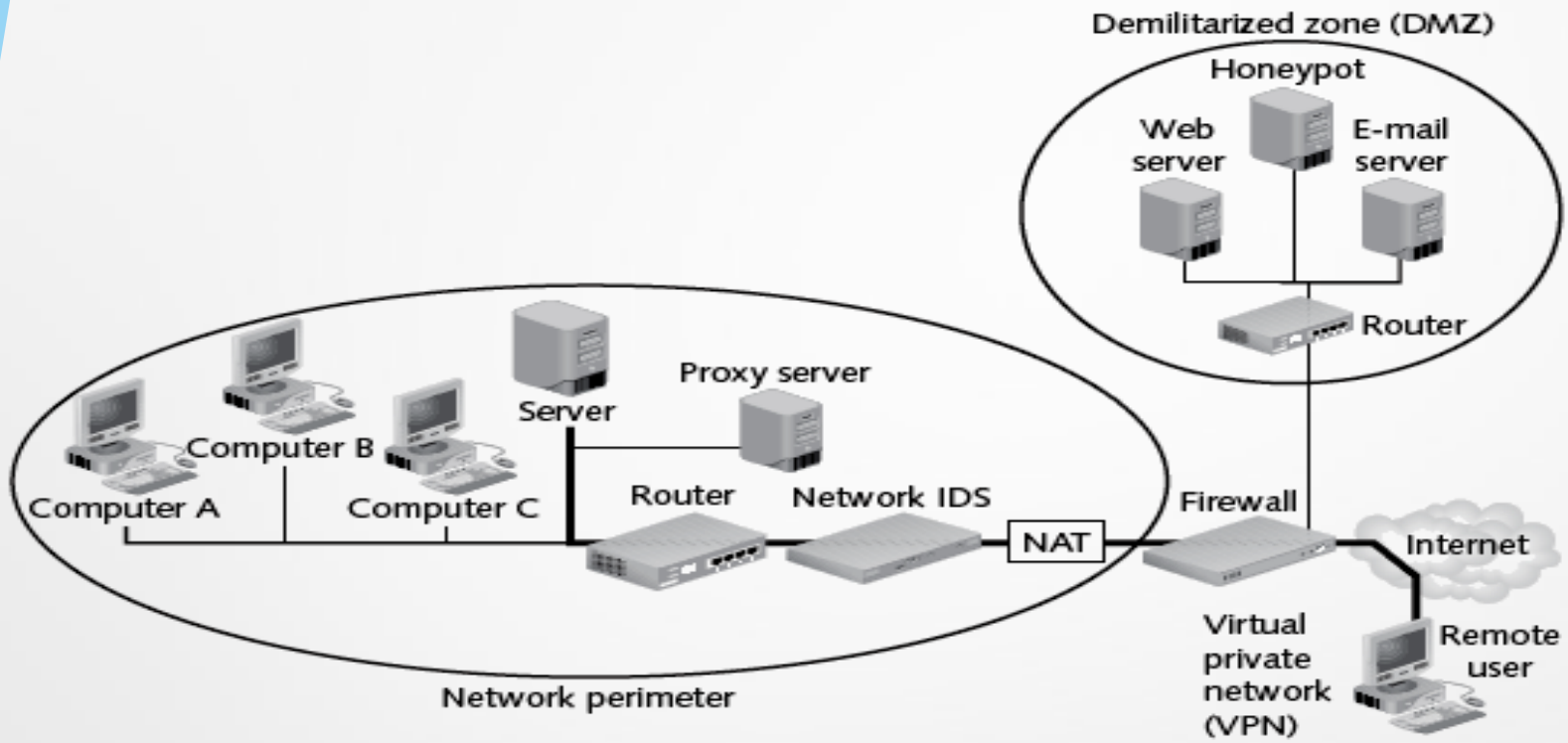


FIgure 5-21 Honeypot

Honeypots → Computer located in a DMZ and loaded with files and software that appear to be authentic, but are actually imitations

- Intentionally configured with security holes
- Goals: Direct attacker's attention away from real targets; Examine the techniques used by hackers

Overview of Existing Security Systems : Secure Socket Layer (SSL)

SSL is used for securing communication between clients and servers. It provides mainly confidentiality, integrity and authentication

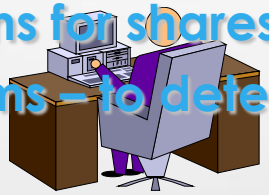
Establish SSL connection - communication protected

Client

WWW Server

Protecting one Computer

- **Operating system hardening is the process of making a PC operating system more secure**
  - **Patch management**
  - **Antivirus software – to protect your pc from viruses**
  - **Antispyware software**
  - **Firewalls – to deter (scare), protect**
  - **Setting correct permissions for shares**
  - **Intrusion detection Systems – to detect intrusions**
  - **Cryptographic systems**



Protecting a Wireless Local Area Network (WLAN)

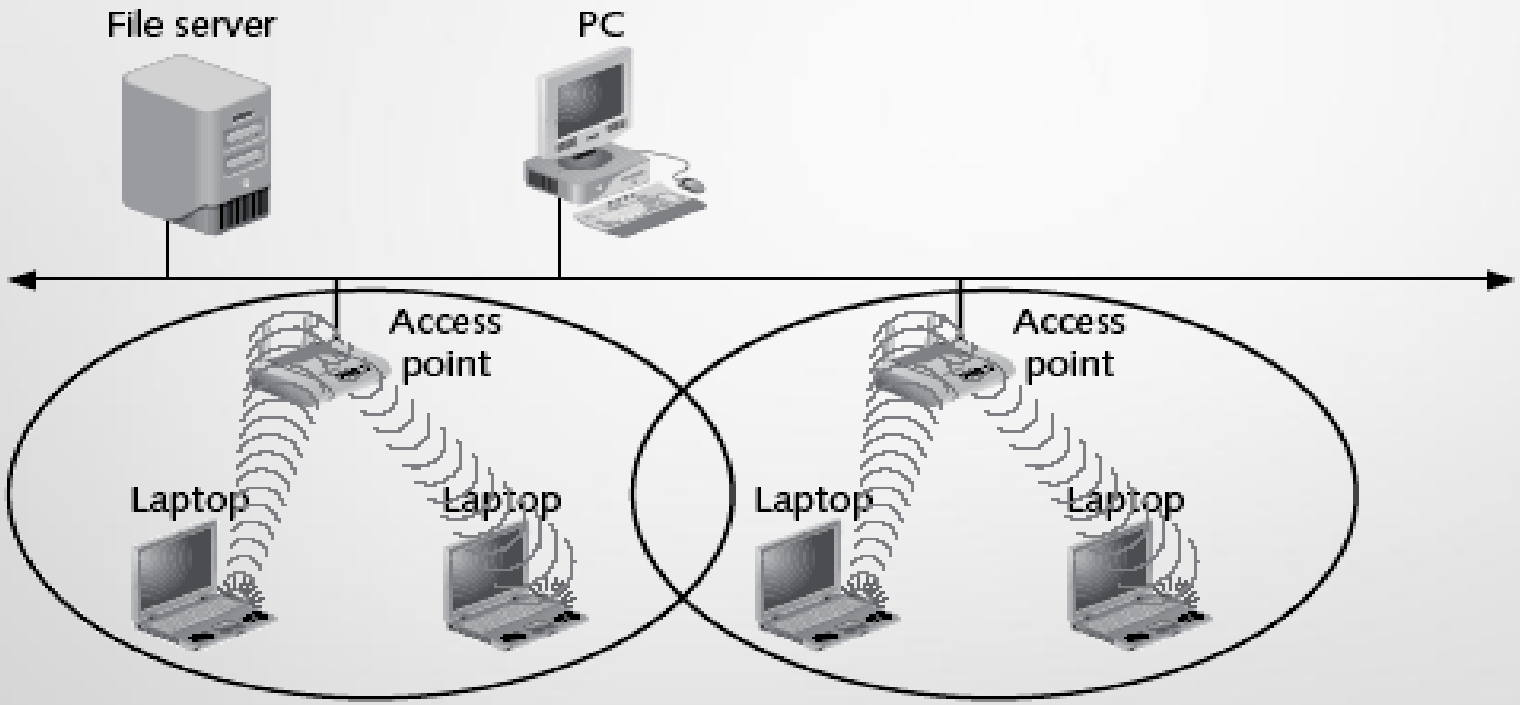


FIgure 5-22 Wireless local area network

Security in a Wireless LAN

- WLANs include a different set of security issues
- Steps to secure:
  - Turn off broadcast information
  - MAC address filtering
  - Encryption
  - Password protect the access point
  - Physically secure the access point
  - Use enhanced WLAN security standards whenever possible
  - Use cryptographic systems