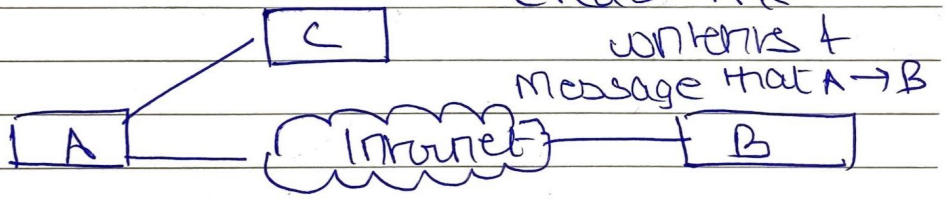
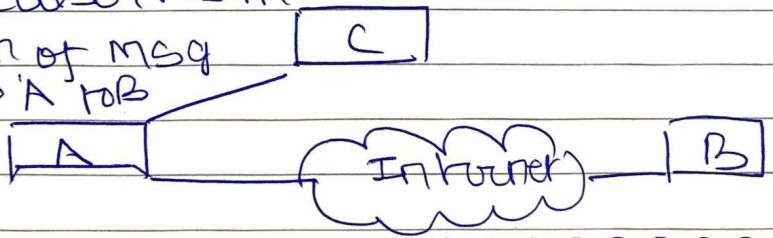
classmate
Date 17/1/23
Page 1

Passive Attacks attends to learn or make use of information from the system but does not affect system resources

1) Release of message content



2) Traffic analysis



4) Man in the middle Attack

It occurs when someone b/w you and the person with whom you are communicating is actually monitoring, capturing & controlling your communication

5) IP Spoofing (IP address spoofing)

In this attack, an attacker use special program to construct IP packets that appear to originate from valid addresses

Password based attack

6) Older applications do not always protect identity information

→ Attacker gain access to the n/w by posing as a valid user with password based access control

7) Sniffer attack/ Packet attack

→ A sniffer is an application in a device that can read, monitor & capture data packets

→ If the packets are not encrypted, a sniffer provide full view of data

→ Encapsulated packets cannot be read until they are encrypted.

8) Phishing

This a practice of sending email from companies in order to induce individuals to reveal personal information such as passwords, credit card, banking info etc

9) DNS spoofing (DNS cache poisoning)

It is a form of computer security in which DNS system introduce causing the nameserver to return an incorrect IP address.

Suppose we had a way of masking of information (encryption) so that the attacker could not extract any inform from the message. he could determine the location & observe the frequency & length of messag-es

Types of Network Layer Attack

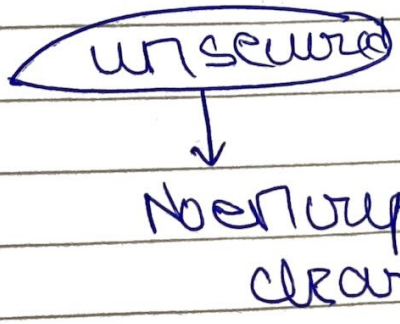
1) Eavesdropping

→ In this commu., occur in an unsecured format

→ Which allows an attacker to read the traffic

→ It is also referred to as sniffing & snooping.

→ It can be improved with strong encryption services



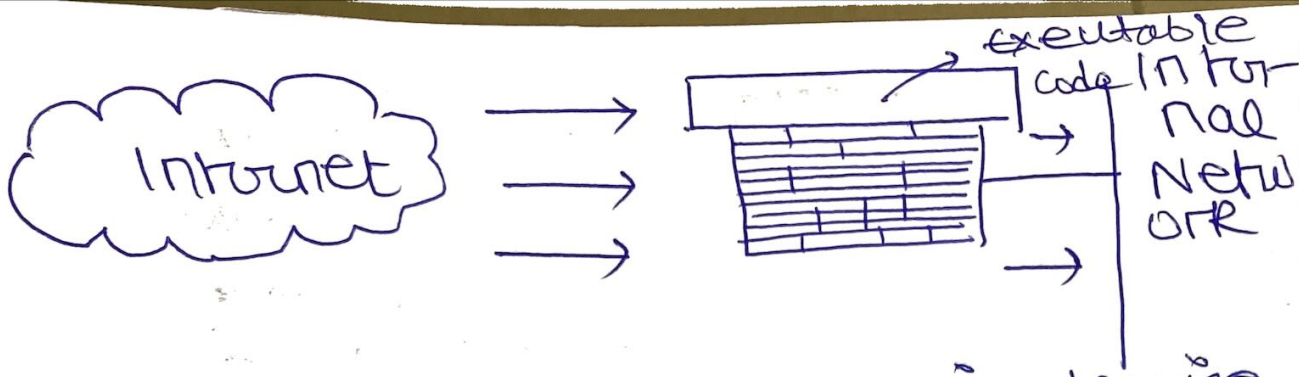
Data Modification

1) After an attacker reads your data the next step is to alter it without the knowledge of sender or receiver.

Compromised Key Attack

→ A key is a secret code or number necessary to interpret secured information

→ An attacker obtains a key is referred to as compromised key.



Firewall is a network securing device that monitors incoming & outgoing traffic & permits or blocks data packets based on a set of security rules. It is basically an executable code run on a dedicated computer that works like a barrier.

(Access Control List) ACL

These works on set of rules that can control between incoming & outgoing traffic.

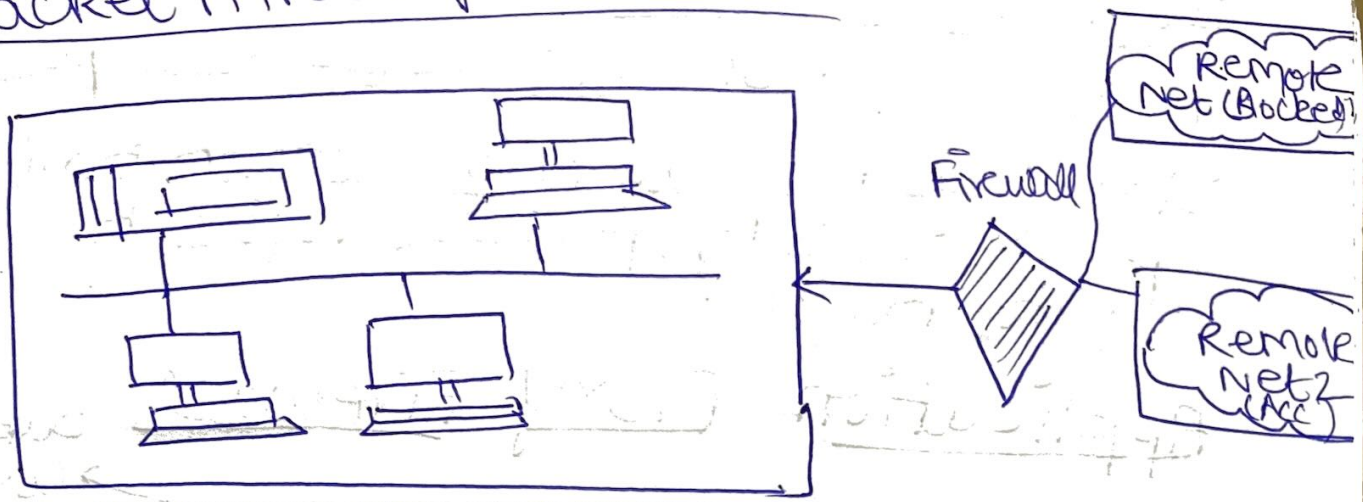
Personal Firewall

It is an application that runs on a personal computer to screen the traffic

Stateless Firewall

It works on upto layer 4 which restricts packets flowing from source to destination

Packet Filtering Firewall



Packets filtered from specific network

A packet filtering firewall controls access to packets on the basis of source & destination IP Address or specific transport layer protocol source & destination

Egress Filtering

It is the practice of monitoring, controlling & restricting traffic, filtering, leaving a network

Ingress

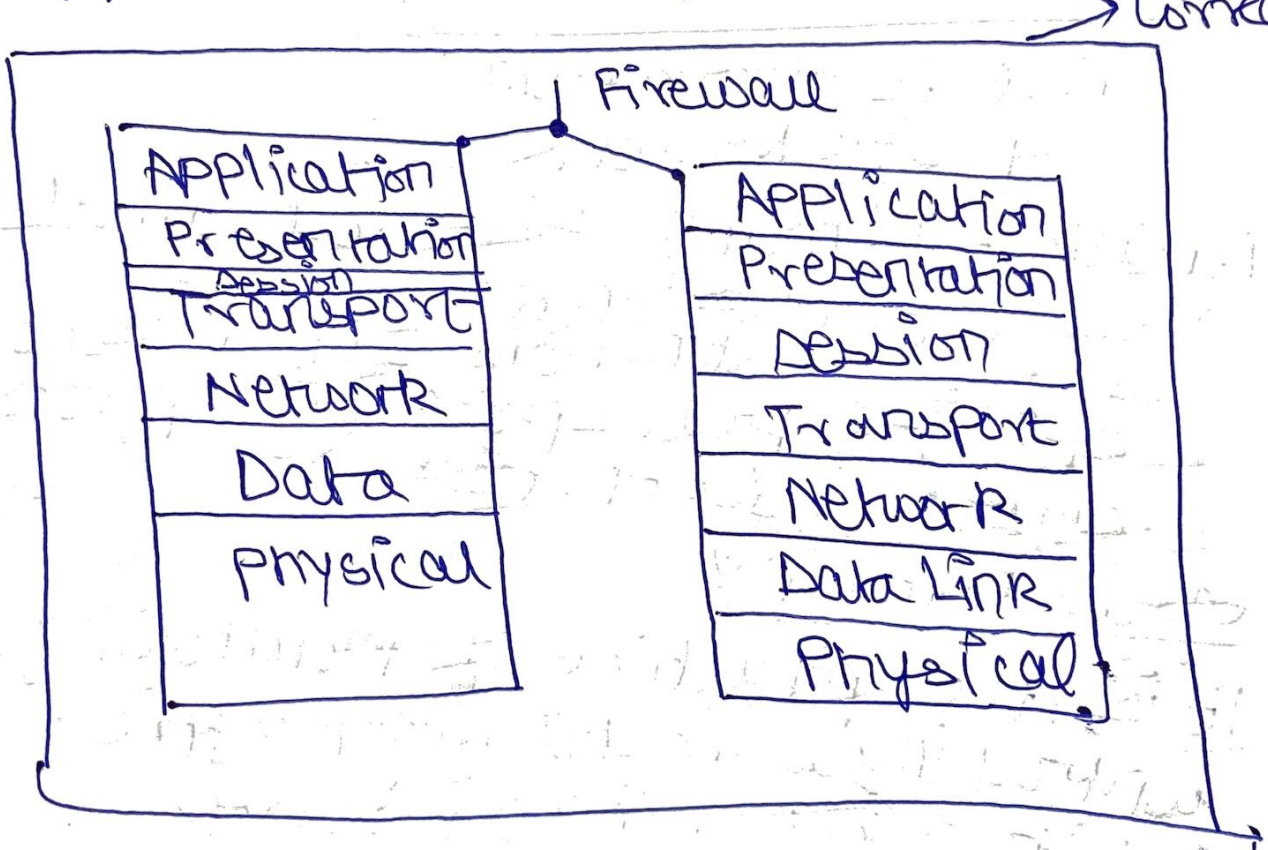
It is a practice of monitoring, controlling & restricting the traffic & entering

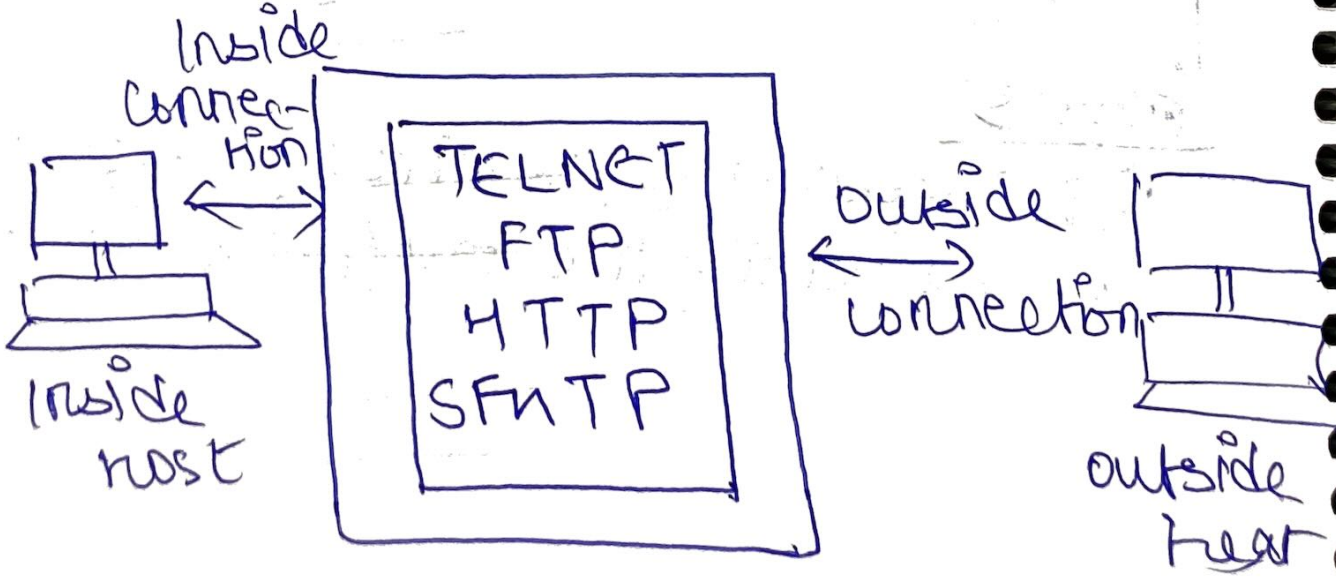
Stateful Firewall

It is based on status of data packs

Stateless Firewall only focuses individual packets using preset rules to filter traffic.

Application Proxy Firewall

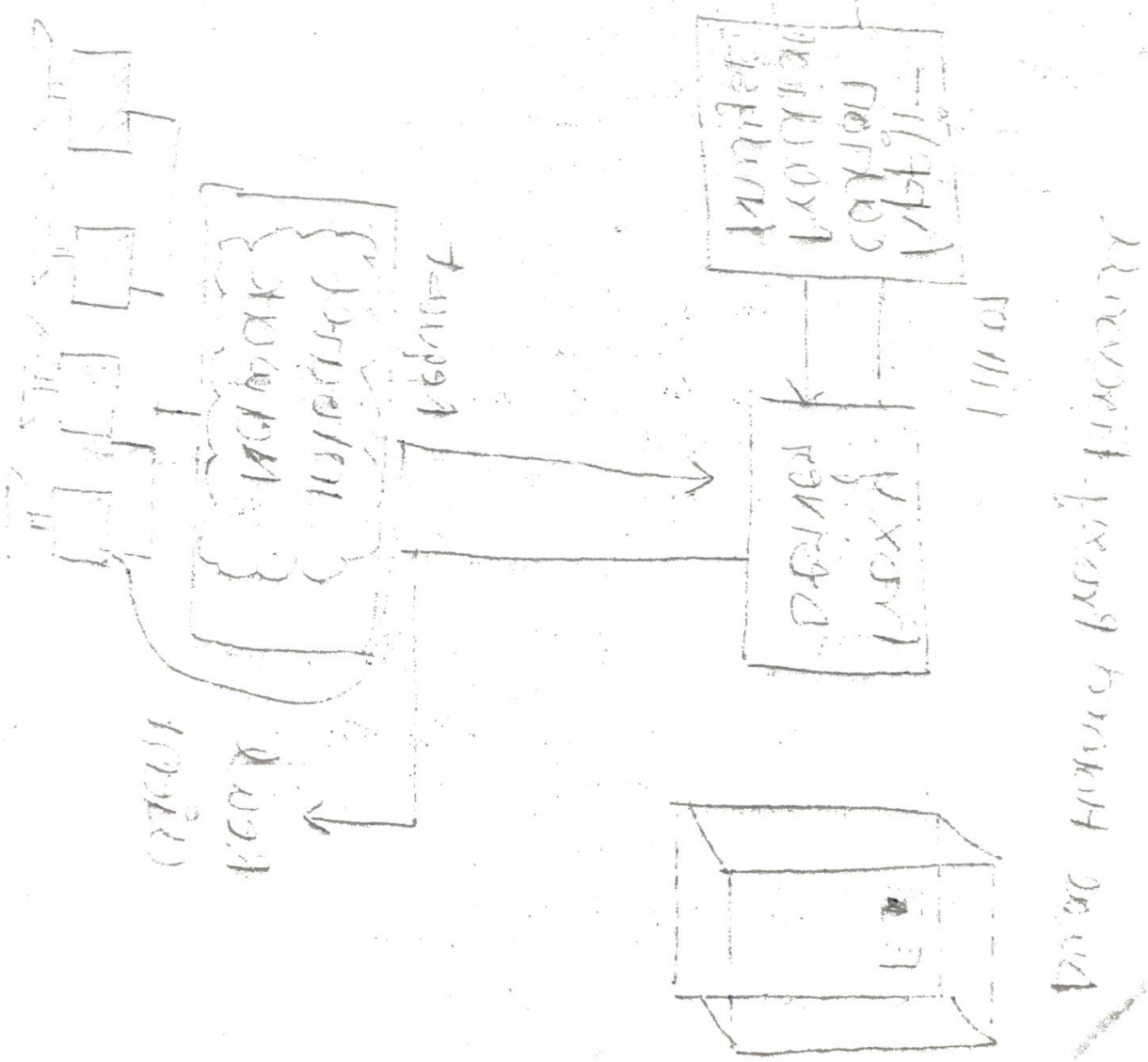


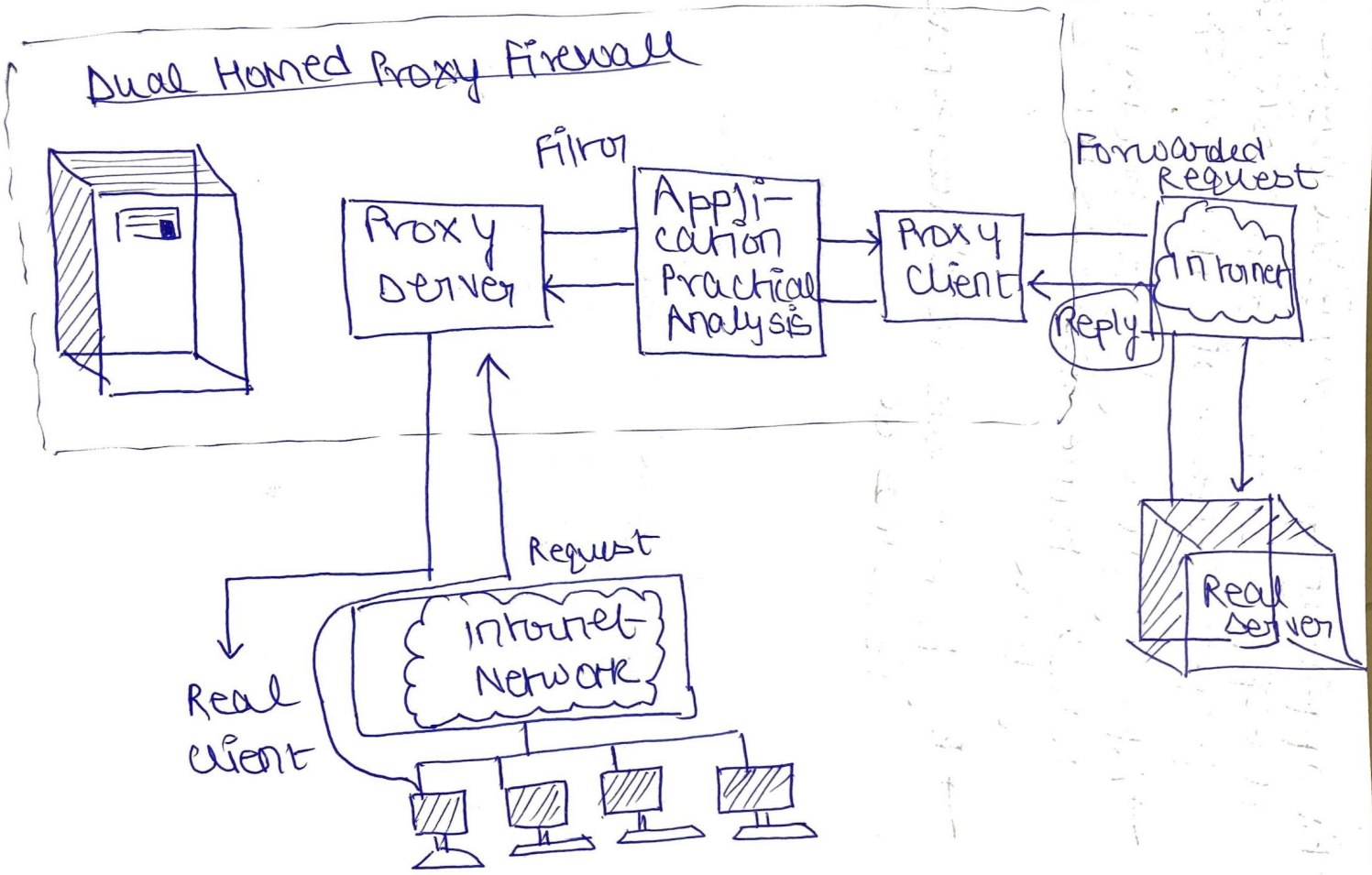


→ An application proxy firewall works on the application layer that simulates proper effects of an application.

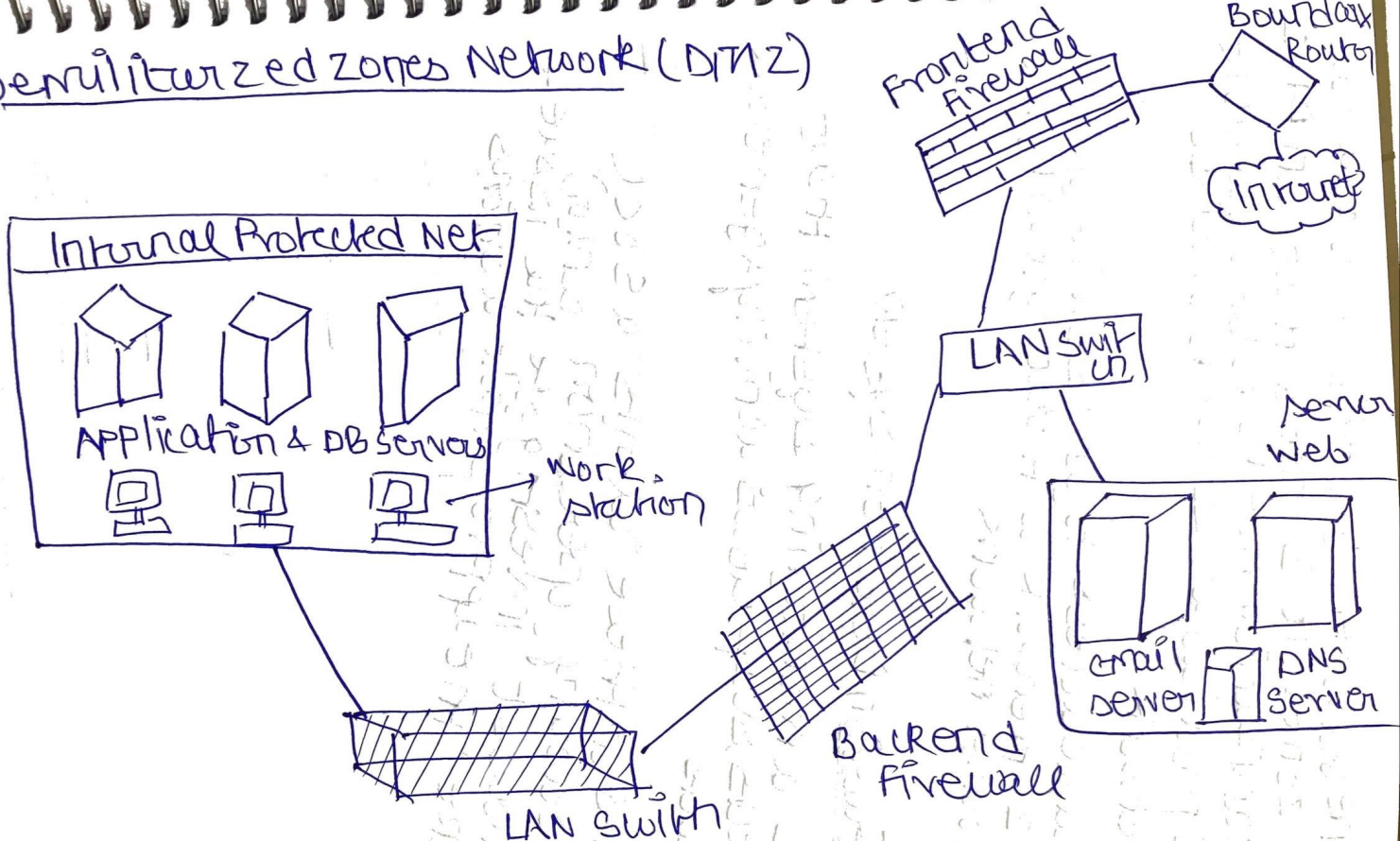
→ A proxy gateway is a two headed device it looks to the inside as if it is the outside

→ By to the outside it responds as it is inside




Dual Homed Proxy Firewall
Filter
Proxy Server
Appli-cation Practical Analysis
Proxy Client
Forwarded Request
Internet
Reply
Request
Internet Network
Real client
Real Server

Demilitarized zones Network (DMZ)



→ The zone between two firewalls are called DMZ zone. It is need that an DMZ organisation needs to be available its particular server to outside network.

→ It allows access to any service on the DMZ network without affecting the internal network

IDS
Intrusion Detection System

→ It is a monitoring system that detects suspicious activity & generate alerts

→ Based on these alerts a SOC (Security operation center) analyst investigate the issue & take the appropriate actions