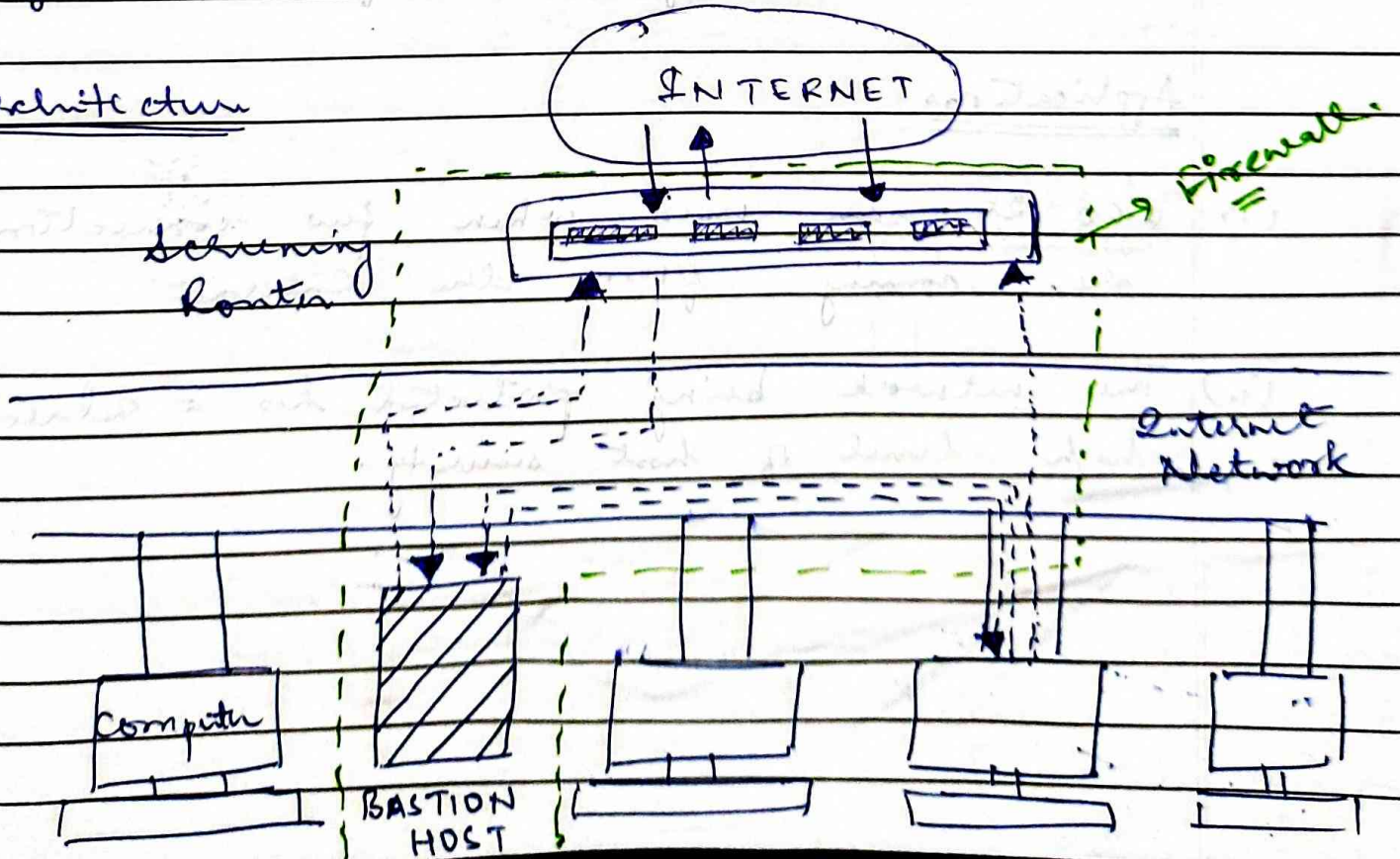
Name - Kulvir Singh
Reg No. - 19BCE2074

Digital Assignment.

A) Screened Host Firewalls.

A firewall which is implemented using a firewall router and proxy server, with the router acting as a frontend to the server. The firewall router first screens off any accesses which are disallowed to a closed network, apart from Web page accesses and secure accesses such as email. The Web accesses are then passed to the proxy server which acts as a frontend to the Web server. That actually dispenses the Web pages.

Architecture



19BCE2074

The figure shows a simple version of a screened host architecture. The bastion host sits on the internal network. The packet filtering on the screening router is set up in such a way that the bastion host is the only system on the internal network that hosts on the Internet can open connections to (for example, to deliver incoming mail). Even then only certain types of connections are allowed. Any external system trying to access internal systems or services will have to connect to this host. The bastion host thus needs to maintain a high level of host security.

Applications

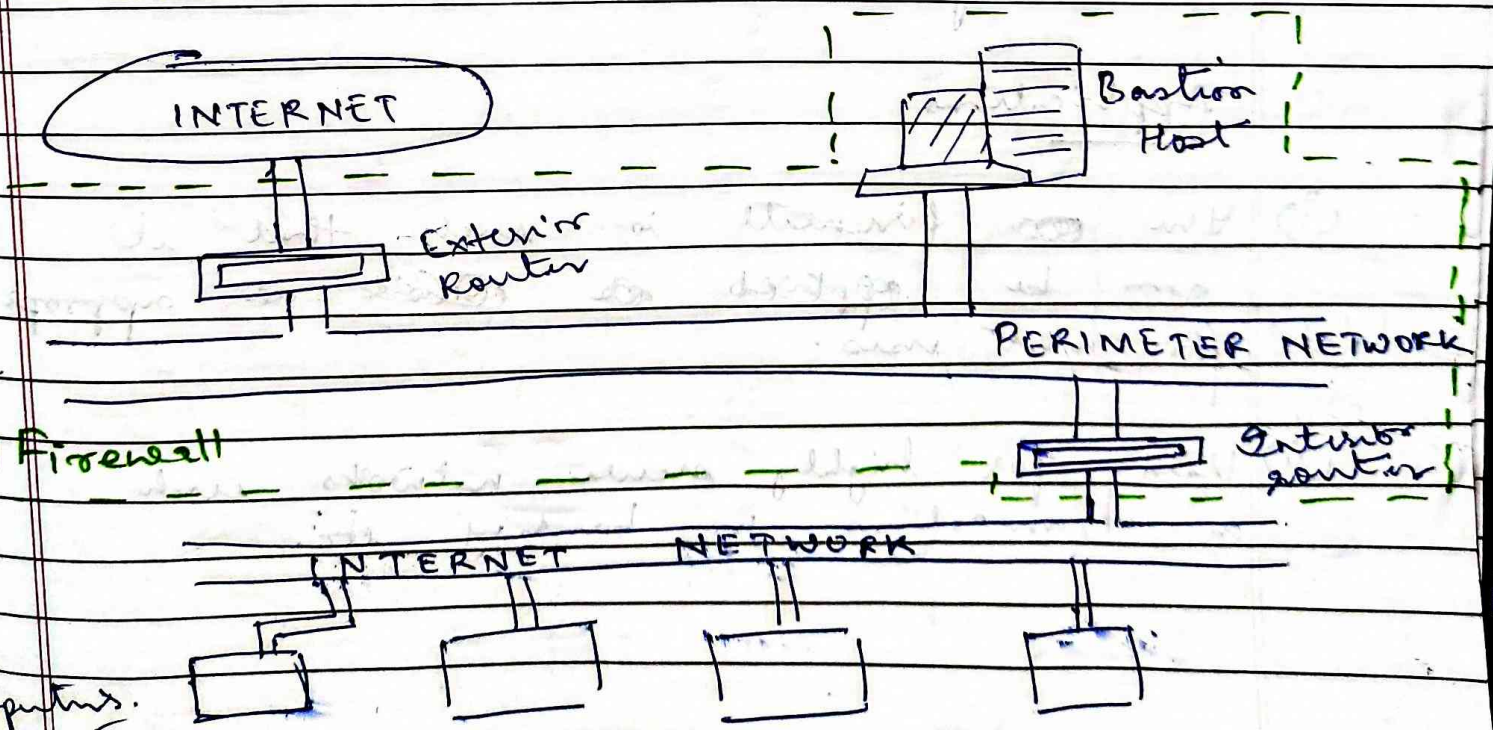
(i) It can used when few connections are coming from the Internet

(ii) The network being protected has a relatively high level of host security:

19BCE2074

B) Screened Subnet Firewalls

In network security a screened subnet refers to the use of one or more logical screening routers as a firewall to define three separate subnets: an external router that separates the external router from a perimeter network, and an internal router that separates the perimeter network from the internal network. The perimeter network, also called a border network or a demilitarized zone (DMZ) is intended for hosting servers (also called Bastion servers hosts) that are accessible from or have access to both internal and external networks.



19BCE2074

With the simplest type of screened subnet architecture, there are two screening routers, each connected to the perimeter net. One sits between the perimeter net and the internal network, and the other sits between the perimeter net and the external network (usually the Internet). To break into the internal network with this type of architecture, an attacker would have to get past both routers. Even if the attacker somehow broke in to the Bastion host, he'd still have to get past the interior router. There is no single vulnerable point that will compromise the internal network.

Applications

(i) The firewall is such that it can be applied as appropriate for most uses.

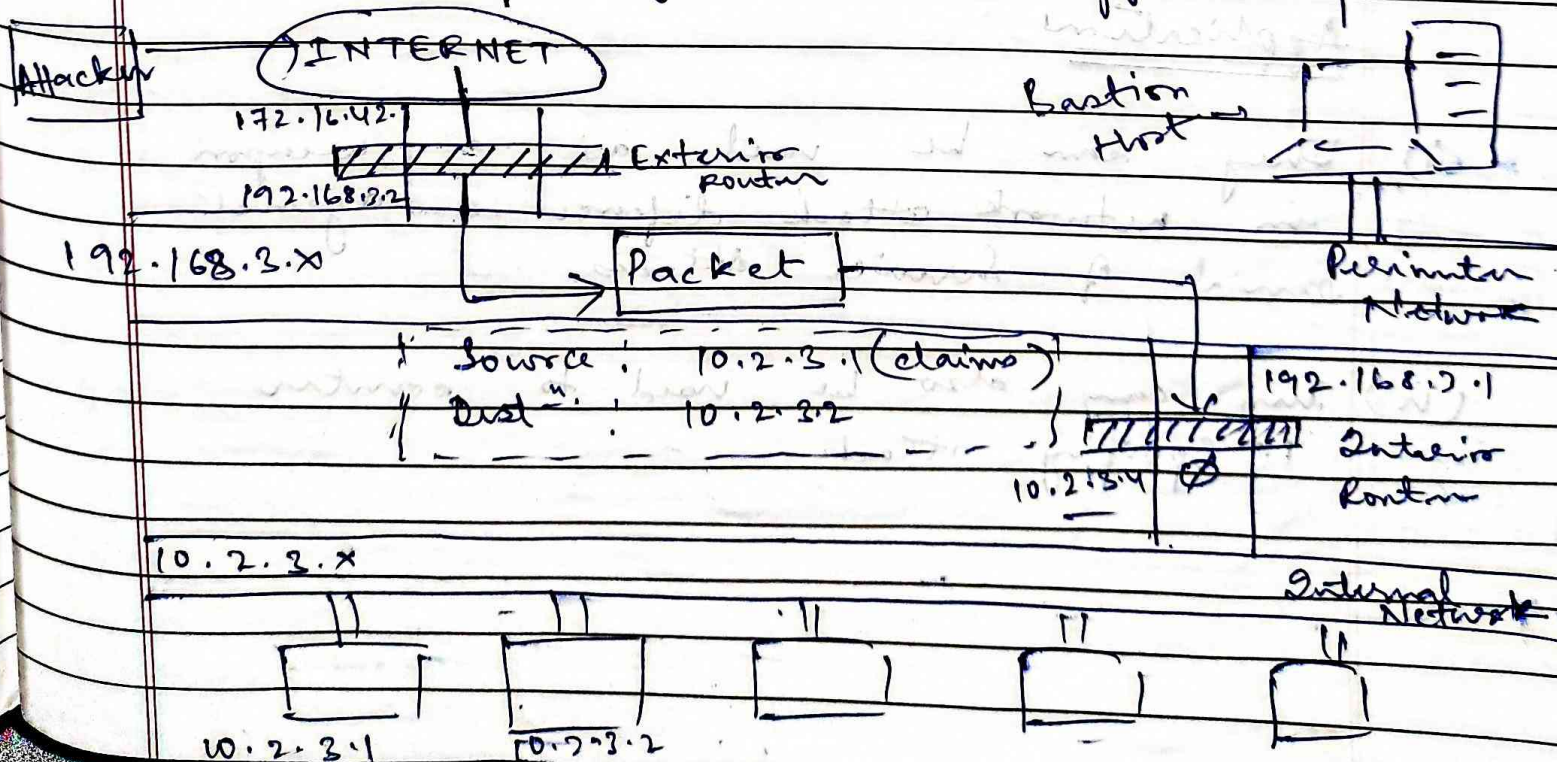
(ii) Used for highly secure networks such as transactions in banking etc.

19BCE2074

classmate
Date
Page

c) Packet Filter Firewalls.

Packet filtering firewalls operate at the network layer (Layer 3) of the OSI model. Packet filtering firewalls make processing decisions based on network addresses, ports or protocols. They are very fast because there is not much logic going behind the decisions they make. They do not store any state information. You have to manually open ports for all traffic that will flow through the firewall. They are not considered to be very secure as they will forward any traffic that is flowing on an approved port.



19BCE2074

Date
Page

The packet filtering firewall filters IP packets based on source and destination IP address, and source and destination port. The packet filter may lack logging facilities, which would make it impractical for an organisation that has compliance and reporting requirements to which they must adhere. Also, because it examines only the packet headers, attackers can bypass the static packet filter with simple spoofing techniques, since the filter cannot tell the difference between a true and a forged address

Applications

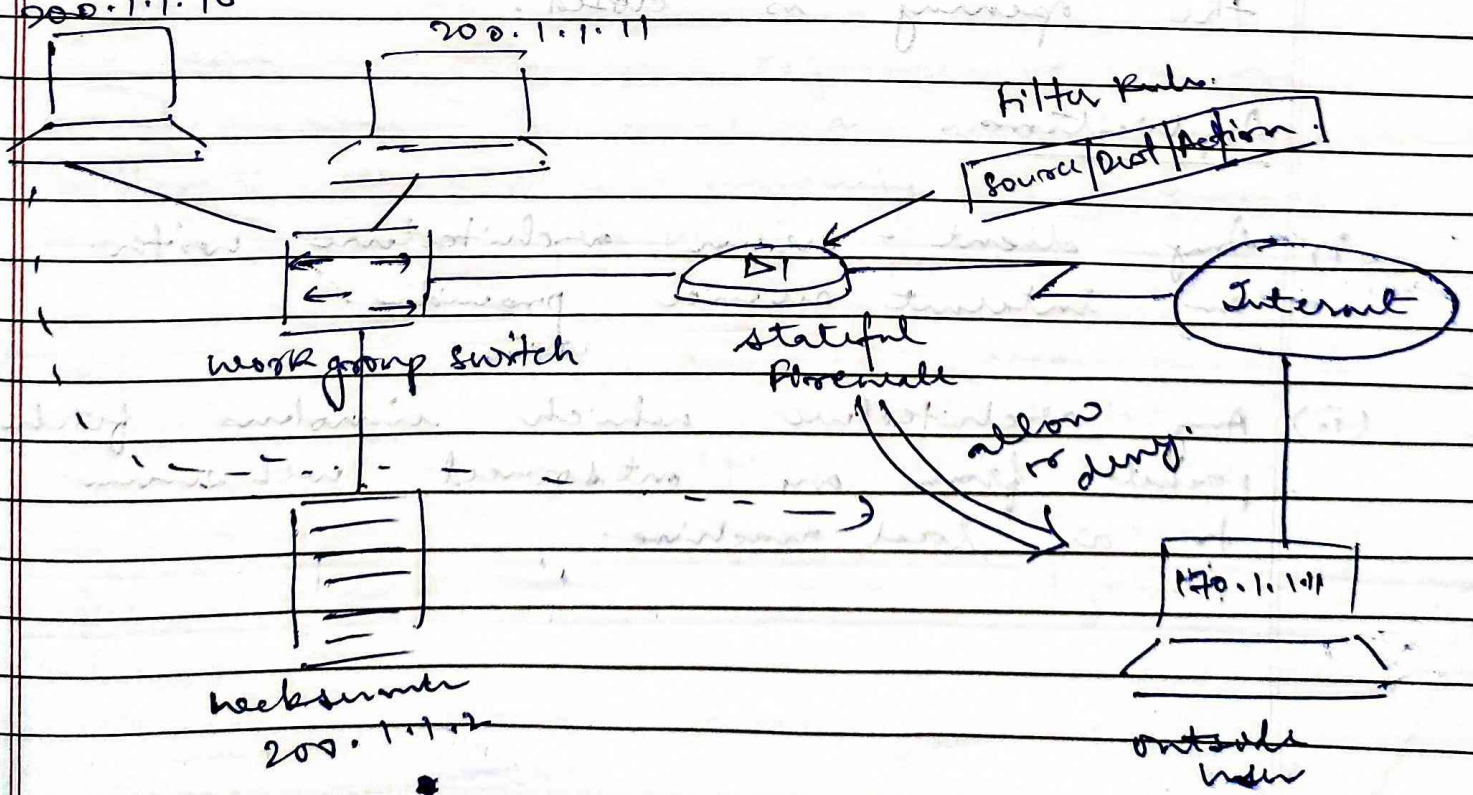
(i) They can be used as a weapon in network attack defence against Denial of Service attacks.

(ii) They can also be used to counter IP Spoofing attacks.

19BCE2074

D) **Stateful Inspection Firewalls**

Stateful inspection firewall is a technology that controls the flow of traffic between two or more networks. Stateful inspection firewalls track the state of sessions and dropping packets that are not a part of a session allowed by a predefined security policy. This is sometimes called session-level protection because they keep state information for each network session and make allowed/denied decisions based on a session stable state table.



19BCE2074

Stateful Inspection is today's choice for the core inspection technology in firewalls. Stateful inspection functions like a packet filter by allowing or denying connections based upon the same types of filtering. However, a stateful firewall also monitors the state of a communication. For example, when you connect to a Web server and that Web server must respond to you, the stateful firewall has the proper access open and ready for the responding connection. When the connection ends, the opening is closed.

Applications:

(i) Any client - server architecture with an internet service provider.

(ii) Any architecture which involves fetching packets from an outsourced web server to a local machine.

Date
Page

E) **Hybrid Firewalls.**

A hybrid firewall may consist of a packet filtering combined with an application proxy firewall or a circuit gateway combined with an application proxy firewall. They contain components of different types of firewalls :-

- packet filtering + MAC layer filtering
- packet filtering + circuit gateway
- packet filtering + proxy server.

Applications

(i) It can be used in organizations which want to make a security improvement without completely removing or replacing its existing firewalls.

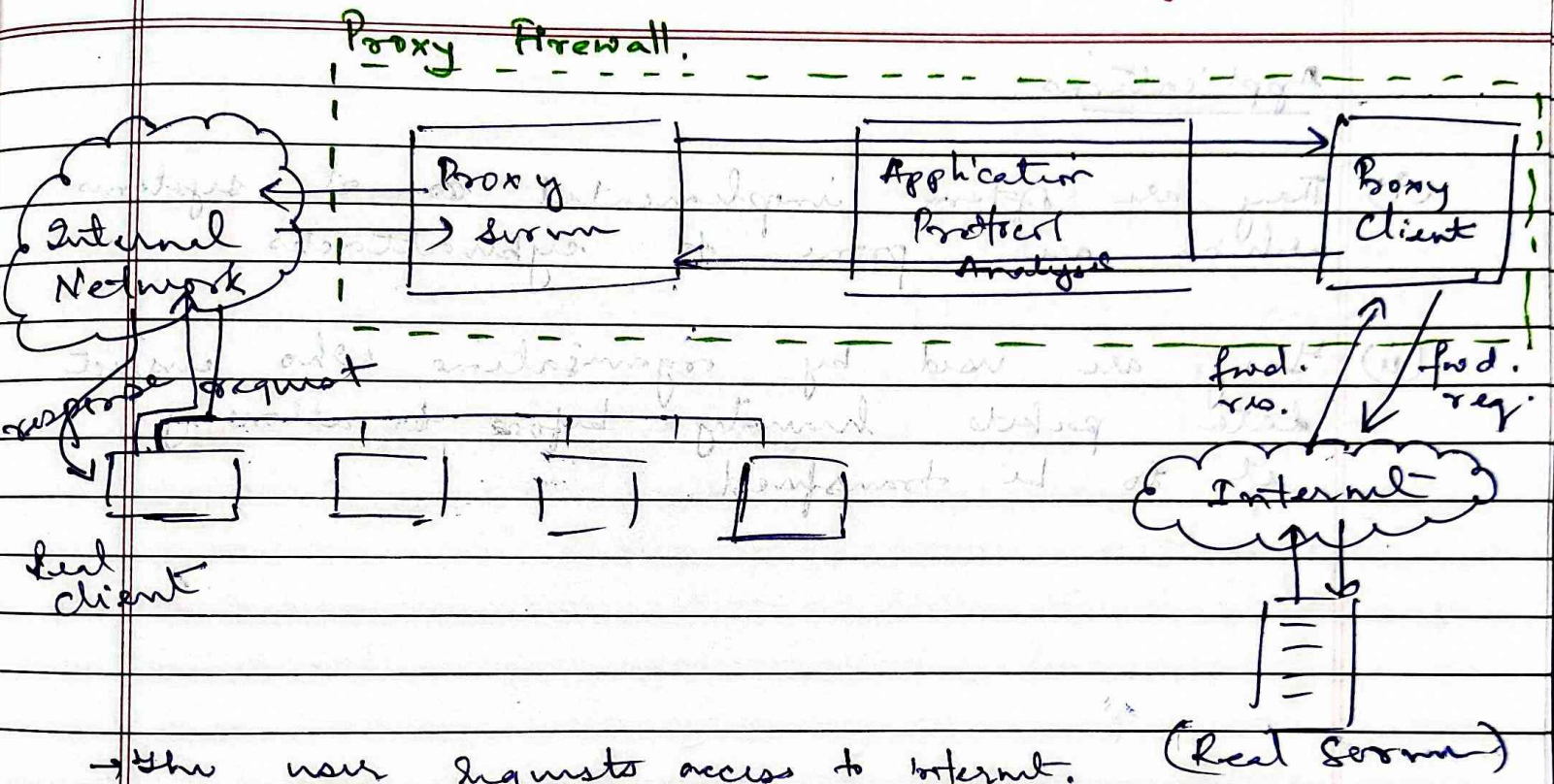
(ii) It can be used anywhere according to requirements of the security architecture and can solve multiple problems due to its architecture comprising of various firewall components mixed together.

19BCE2074

F) Proxy Server Firewall

A proxy firewall is the most secure form of firewall, which filters messages at the application layer to protect network resources. A proxy firewall also known as an application firewall or a gateway firewall, limits the applications that a network can support, which increases security levels but can affect functionality and speed. A proxy server provides a gateway or intermediary between computers and servers on the internet to secure the data that goes in and out of a network. It determines which traffic should be allowed and denied and analyzes incoming traffic to detect signs of a potential cyber attack or malware.

19BCE2074



→ The user requests access to internet. The user's comp. attempts to create a session between them and the server, sending a synchronize message packet from their IP address to the server's IP address. The proxy firewall intercepts the request and if its policy allows replies with a syn-ack packet from the requested server's IP. When the SYN-ACK packet is received by the user's IP it sends one final ACK packet to server's IP. 3 way handshake is carried out and data transfer takes place.

19BCE2074

Applications

(i) They are often implemented at systems which are prone to cyberattacks.

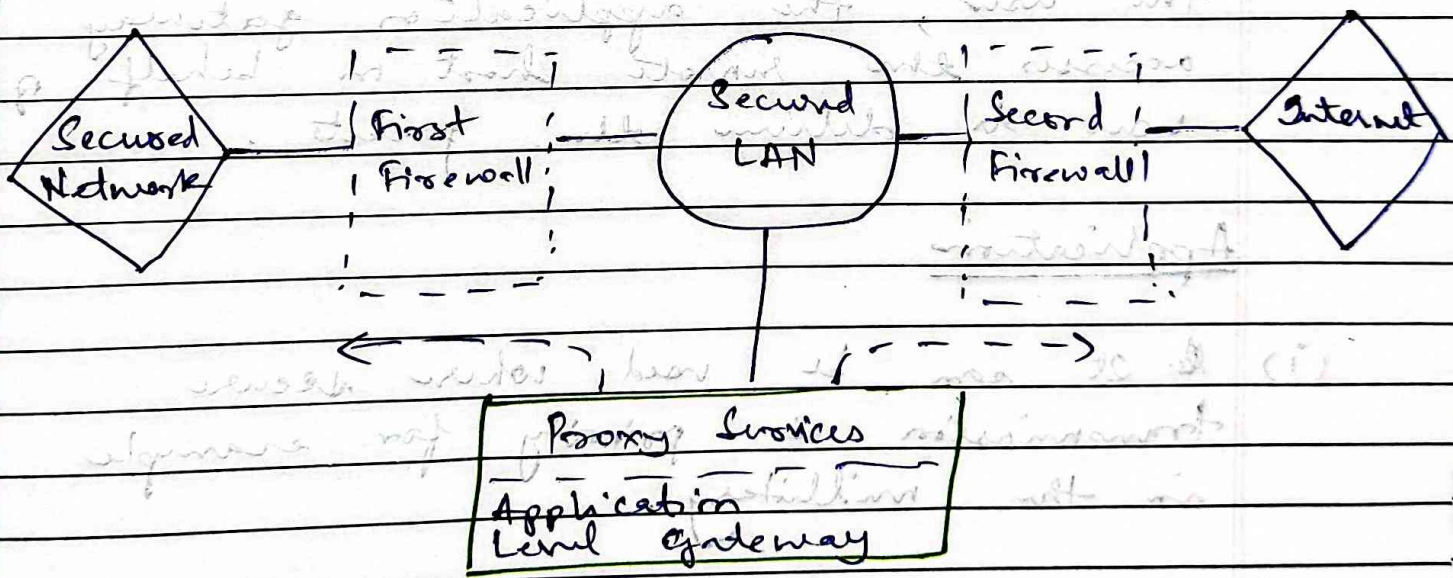
(ii) They are used by organisations who inspect data packets heavily before allowing it to be transfred.

19BLE2074

classmate
Date
Page

6) Application level (gateway) firewalls.

Application proxies are configured in multi-homed arms and they are often used instead of router-based traffic controls, to prevent traffic controls, to prevent traffic from passing directly between networks. Application proxy-based firewalls function at the application level. At this level, you can block or control traffic generated by applications.



19BCE2074.

The architecture is described in the following steps written below :-

Step 1 : User contacts the application gateway using a TCP/IP application such as HTTP.

Step 2 : The application gateway asks about the remote host with which the user wants to establish connection. It also asks for the user id and password that is required to access the services of the application gateway.

Step 3 : After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.

Applications

(i) It can be used when secure transmission is priority for example in the military.

(ii) It can be used where system admins alter permissions and validate requests.