Unit 4

Q) Firewall characteristics

All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are

possible.
Only authorized traffic, as defined by the local security policy, will be allowed to pass.
Various types of firewalls are used, which implement various types of security policies.
The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system. ~~This implies that use of a trusted~~
Four techniques that firewall use to control access and enforce the site's security policy is as follows:-

1) Service control: determines the type of internet services that can be accessed, inbound or outbound. The firewall may filter traffic on this basis of IP address and TCP port number, may provide proxy software that receives and interprets each service request before passing it on, or may host the server software

itself, such as web or mail service.

2) Direction control - determines the direction in which particular service request may be initiated and allowed to flow through the firewall.

3) User control - controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from extra external users; the latter requires some form of secure authentication technology.

4) Behavior control - controls how particular services are used. For example, the firewall may filter

e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

Capabilities of firewall

A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.

A firewall provides a location for monitoring security related events. Audits and alarms can be implemented on the firewall system.

A firewall is a convenient platform for several internet functions that are not security related.

A firewall can serve as the platform for IPsec.

5] Types of firewalls

1) Packet filtering firewalls
2) Circuit level Gateway firewalls
3) Application level Gateway firewalls
4) Stateful Multilayer Inspection firewalls

Packet filtering firewall

Packet filtering firewalls are normally deployed on the routers which connect the internal network to internet Packet filtering firewalls can only be implemented on the Network layer of OSI Model.

Packet filtering firewalls work on the basis of rules defined by Access control lists. They check all the packets and screen them against the rules defined by the Network Administrator as per the ACLs. If in case, any packet does not meet the criteria then that

packet is dropped and logs are updated about this information.
Administrators can create their ACLs on the basis of Address, Protocols and Packet attributes.

Advantage:-
The biggest advantage of Packet filtering firewalls is cost and lower resource usage. Best suited for smaller networks.

Disadvantage:
Packet-filtering firewalls can work only on the Network layer and these firewalls do not support complex rule based models. Also vulnerable to spoofing in some cases.

2) Circuit level Gateway firewalls:-
Circuit level gateways are deployed at the session layer

of the OSI model and they monitor sessions, like TCP three way handshake to see whether a requested connection is ligitimate or not.
Major scanning happens before the connection is established.
Information sent to a computer outside the network through a circuit-level gateway appears to have originated from the Gateway. This helps in creating a stealth cover for the private network from outsiders.

Advantage:
Circuit level gateways are comparatively inexpensive and provide anonymity to the private network.

Disadvantage:
Circuit level Gateways do not filter individual packets. After establishing a

connection, an attacker may take advantage of this.

Application level Gateway Firewalls

Application level gateways work on the Application layer of the OSI model and provide protection for a specific Application layer Protocol. Proxy server is the best example of Application level Gateways firewalls.

Application level gateway would work only for the protocols which is configured. For example, if we install a web proxy based firewall then it will only allow HTTP Protocol data. They are supposed to understand application specific commands such as HTTP: GET and HTTP: POST as they are developed deployed on the Application layer, for a specific Protocol.

Application level firewalls

can also be configured as caching servers which in turn increase the network performance and makes it easier to log traffic.

Stateful Multilayer Inspection firewall

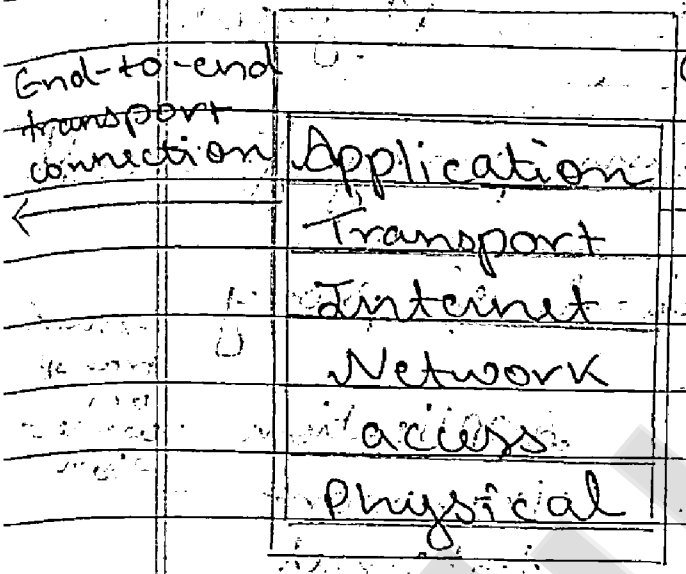
Stateful multilayer Inspection firewall is a combination of all the firewalls that we have studied till now.

They can filter packets at Network layer using ACLs, check for the legitimate sessions on the session layers and they also evaluate packets on the Application layer (AL (or).

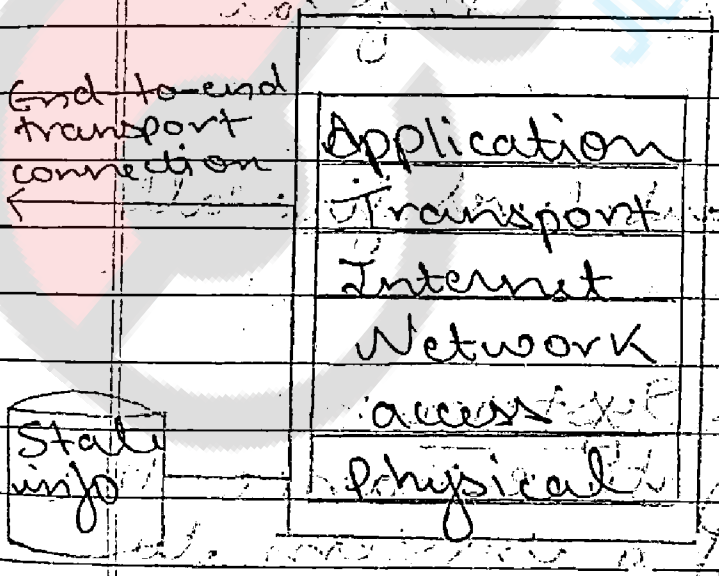
Stateful Multilayer Inspection firewall can work on a Transparent mode allowing direct connections between the client and the server which was earlier not possible.

PAGE NO.
DATE ../../..

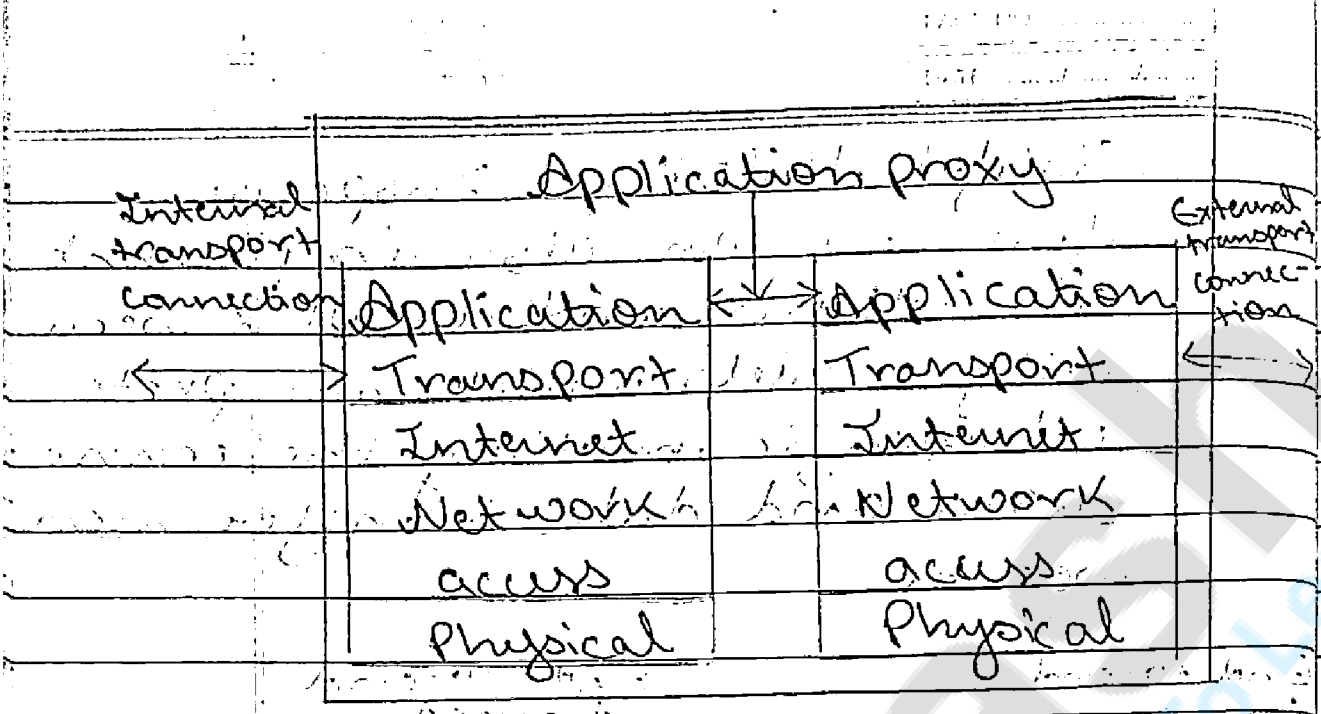
Stateful Multilayer Inspection firewall can also implement algorithms and complex security models which are protocol specific, making the connections and data transfer more secure



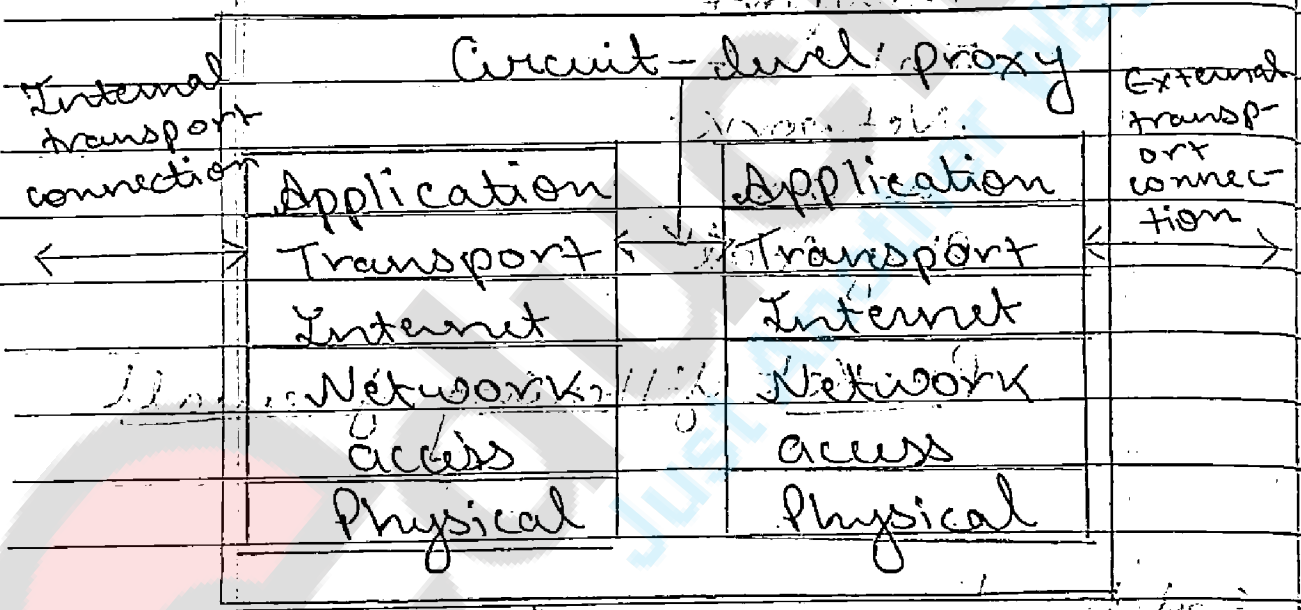
Packet filtering firewall



Stateful inspection firewall



Application proxy firewall



Circuit-level firewall

8] Trusted Systems:-

One way to enhance the ability of a system to defend against intruders

and malicious programs is to implement trusted system

▷ Data access control
- Through the user access control procedure (log on), a user can be identified to the system
- Associated with each user, there can be a profile that specifies permissible operations and file accesses.
- The operation system can enforce rules based on the user profile

▷ General modes of access control
- Access matrix
- Access control list
- Capability list

▷ Access matrix :- Basic elements of the model
- Subject : An entity capable of accessing objects, the concept of subject equates with that of process
- Object : Anything to which access is controlled eg files,

(no groups)
- Access rights: The operation which an object is allowed by a subject (eg. write, execute)

* Access control list
- The access control list lists users and their permitted access rights
- The list may contain a default or public entry

* Capability list
- A capability ticket specifies authorized objects and operations for a user
- Each user has a number of tickets

* Trusted Systems
- Protection of data and resources on the basis of levels of security (eg. military)
- Users can be granted clearances to access certain categories of data

▶ Multilevel security
- Definition of multiple categories or levels of data.

▶ A multilevel secure system must enforce:
- No read up: A subject can only read an object of less or equal security level
- No write down: A subject can only write into an object of greater or equal security level

▶ Reference Monitor
- controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on basis of security parameters
- The monitor has access to a file (security kernel database) that lists all
- The monitor enforces the security rules (no read up, no write down)

▶ Properties of the Reference Monitor

- Complete mediation: Security rules are enforced on every access
- Isolation: The reference monitor and database are protected from unauthorised modification
- Verifiability: The reference monitor's correctness must be provable (mathematically)

Q] Firewall Architectures :-

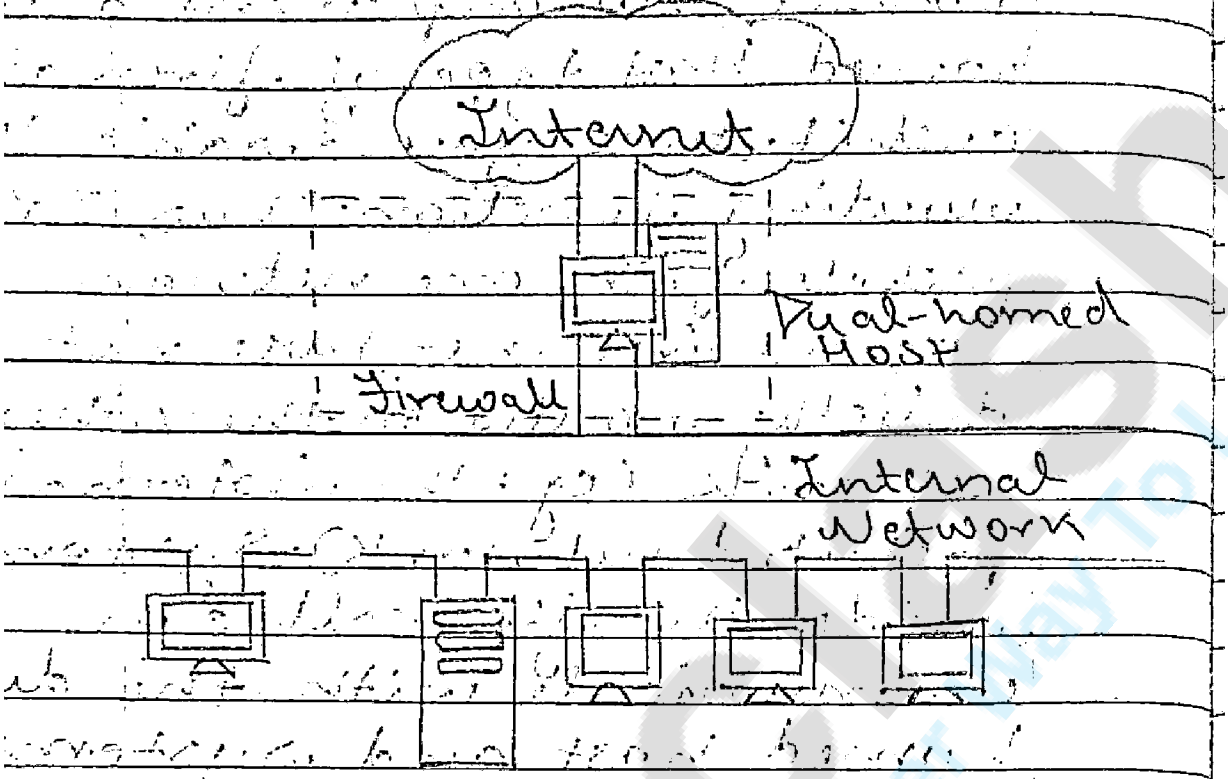
1) Dual-Homed Host Architecture :-

A dual-homed host architecture is built around the dual-homed host computer, a computer which has atleast two network interfaces. Such a host could act as a router between the networks these interfaces are attached to; it is capable of routing IP packets from

one network to another. However, to implement a dual-homed host type of firewalls architecture, you disable this routing function. Thus, IP packets from one network (eg. the internet) are not directly routed to the other network (eg: the internal, protected network). Systems inside the firewall can communicate with the dual-homed host and systems outside the firewall (on the internet) can communicate with the dual-homed host, but these systems can't communicate directly with each other. IP traffic between them is completely blocked. The network architecture for a dual-homed host firewall is pretty simple. The dual homed host sits between and is connected to the Internet and the internal network

Scanned by CamScanner

Dual-homed host architecture



Dual-homed hosts can provide a very high level of control. If you aren't allowing packets to go between external and internal networks at all, you can be sure that any packet on the internal network that has an external source is evidence of some kind of security problem. In some cases, a dual-homed host will allow you to reject connections that claim to be for a particu-

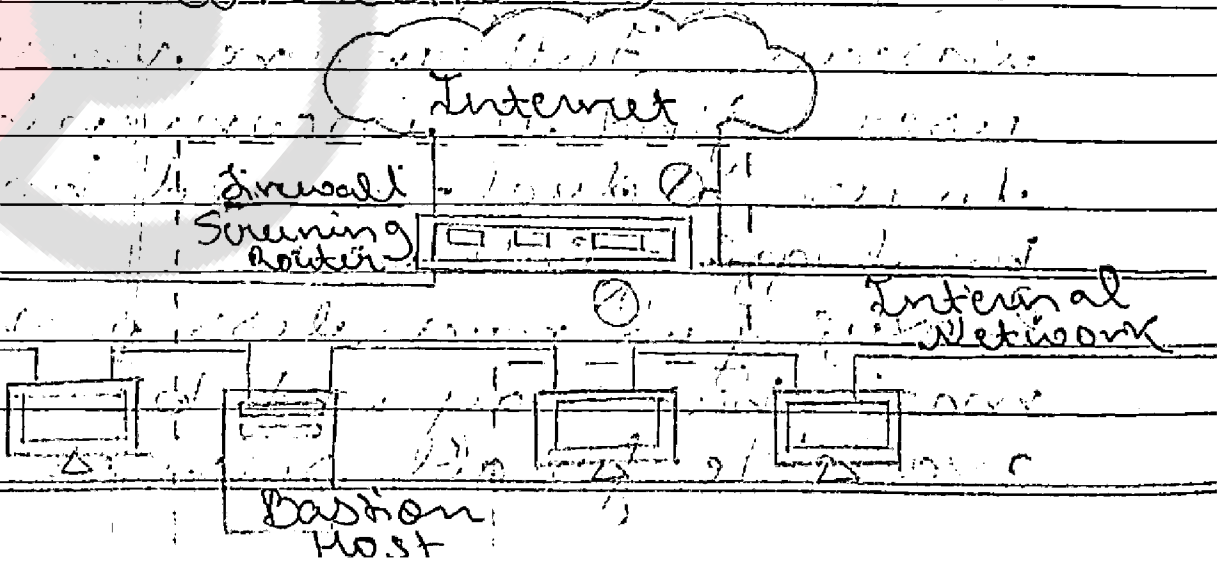
for service but that dont actually contain the right kind of data. A packet filtering system, on the other hand, has difficulty with this kind of control. However, it takes considerable work to consistently take advantage of the potential advantages of dual-homed hosts.

A dual-homed host can only provide services by proxying them, or by having users log into the dual-homed host directly. User accounts present significant security problems by themselves. They present special problems on dual-homed hosts, where they may unexpectedly enable services you consider insecure. Furthermore, most users find it inconvenient to use a dual-homed host by logging into it.

Proxying is much less problematic, but may not be available for all services

you're interested in.

2) Screened Host Architecture
Whereas a dual-homed host architecture provides services from a host that's attached to multiple networks (but has routing turned off), a screened host architecture provides services from a host that's attached to only the internal network, using a separate router. In this architecture, the primary security is provided by packet filtering. (For example, packet filtering is what prevents people from going around proxy servers to make direct connections.)



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 email). 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. The packet filtering also permits the bastion host to open allowable connections (what is "allowable" will be determined by your site's particular security policy) to the outside world.

The packet filtering configuration on the screening

router may do one of the following:

- Allow select internal hosts to open connections to hosts on the Internet for certain services (allowing those services via packet filtering)
- Disallow all connections from internal hosts (forcing those hosts to use proxy services via the bastion host)

You can mix and match these approaches for different services; some may be allowed directly via packet filtering, while others may be allowed only indirectly via a proxy. It all depends on the particular policy your site is trying to enforce.

Because this architecture allows packets to move from the Internet to the internal network at

may seem more risky than a dual-homed host architecture, which is designed so that no external packet can reach the internal network. In practice, however, the dual-homed host architecture is also prone to failures that let packets actually cross from the external network to the internal network. (Because this type of failure is completely unexpected, there are unlikely to be protections against ~~that~~ attacks of this kind.) Furthermore, it's easier to defend a router, which provides a very limited set of services, than it is to defend a host. For most purposes, the screened host architecture provides both better security and better usability than the dual-homed host architecture. Compared to other architecture, there are some disadvantages to the

screened host architecture. The major one is that if an attacker manages to break in to the bastion host, there is nothing left in the way of network security between the bastion host and the rest of the internal hosts. The router also presents a single point of failure; if the router is compromised, the entire network is available to an attacker.

3) Screened Subnet Architecture

The screened subnet architecture adds an extra layer of security to the screened host architecture by adding a perimeter network that further isolates the internal network from the internet. By their nature, bastion

PAGE NO.....
DATE ...../...../.....

hosts are the most vulnerable machines on your network. Despite your best efforts to protect them, they are the machines most likely to be attacked, because they're the machines that can be attacked by, as in a screened host architecture, your internal network is wide open to attack from your bastion host, then your bastion host is a very tempting target. There are no other defenses between it and your other internal machines. If someone successfully breaks into the bastion host in a screened host architecture, he's hit the jackpot. By isolating the bastion host on a perimeter network, you can reduce the impact of a break-in on the bastion host. It is no longer an instantaneous jackpot, it gives an intruder some access, but not all of

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 into the bastion host, he'd still have to get past the internal router. There is no single vulnerable point that will compromise the internal network. Some sites go so far as to create a layered series of perimeter nets between

the outside world and their interior network. less trusted and more vulnerable services are placed on the outer perimeter nets, farthest from the interior network. The idea is that an attacker who breaks into a machine on an outer perimeter net will have a harder time successfully attacking internal machines because of the additional layers of security between the outer perimeter and the internal network. This is only true if there is actually strong meaning to the different layers, however; (e.g. if the configurations between each layer address the same vulnerabilities in all layers, the additional layers don't provide any additional security.

- Screened subnet architecture (using two routers)