Firewalls:-

1. It is a network security system that monitors and controls incoming and outgoing traffic based on some predefined security rules.

Firewall design principles:-

1. Developing Security policy.
2. Simple design.
3. choosing right device.
4. layered defense.
5. consider Internal Threats.

2. It prevents unwanted incoming data from entering into our system.

Developing Security policy:-

1. according to our clients requirements.
2. Monitor the incoming traffic.

Simple Design:-

1. Easy to maintain.
2. New updates can be easily done.

Choosing right device:-

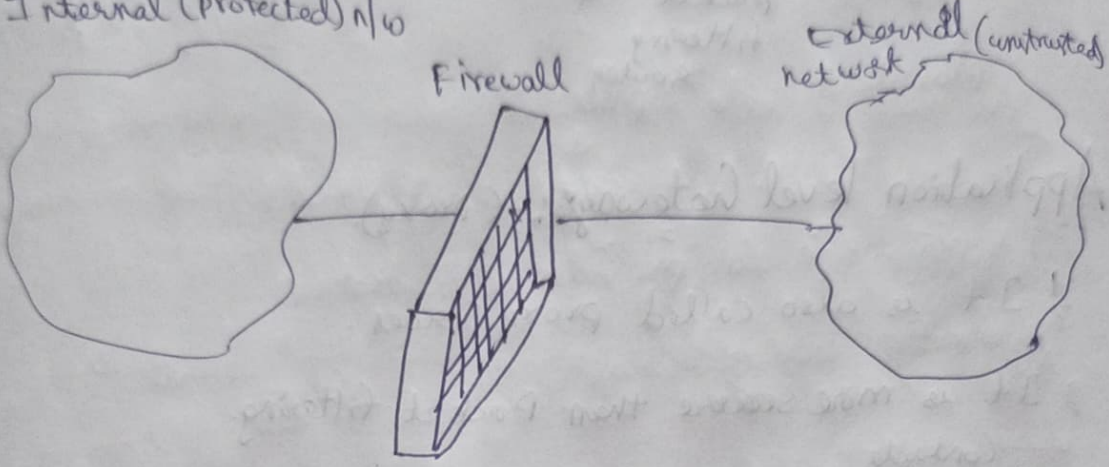
1. while desiging a firewall, the system should be well-secured.
2. Not use outdated systems.

Layered defence:-

1. The design should have multilayer defense.

Consider Internal Network:-

1. We have to consider the internal threats.
2. Analyze the internal threats and design the firewall.



Types of Firewalls:-

1. Packet Filtering.
2. Application-level gateways
3. Circuit-level gateways

Packet Filtering Firewall:-

1. It applies set of rules on each incoming packet and forward the packet if rules are obeyed otherwise discarded.

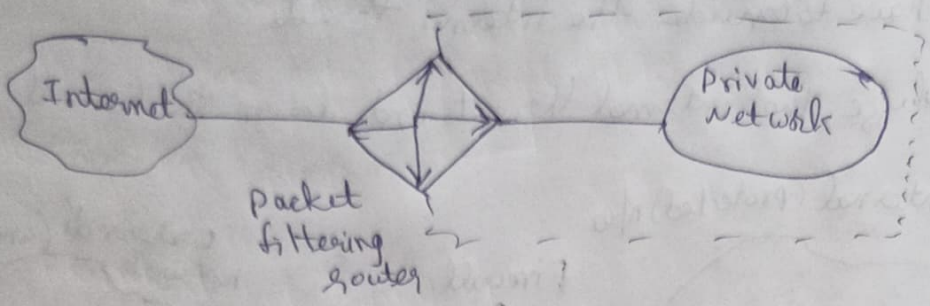
Rules for packet filtering

1. Based on Source I/P.
2. destination I/P.
3. Protocols and Ports

It also maintain a filtering Table.

3 Simple but less secure.

4 It is the faundation of every firewall system.



Application level Gateways :- (Proxy).

1 It is also called proxy server.

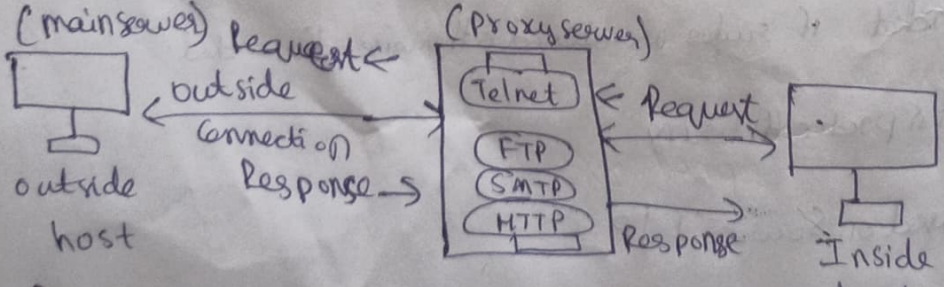
2 It is more secure than Packet filtering.

3 Contacts user by TCP/IP protocols

(TELNET, FTP, SMTP, HTTP).

4 A user contacts the gateways to access some service, provides details of the service, remote host and authentication details.

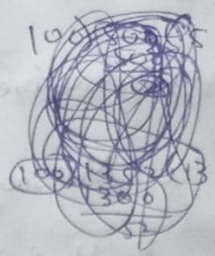
5 If the gateway does not implement the proxy code for a specific application, then it is not supported and cannot be used.



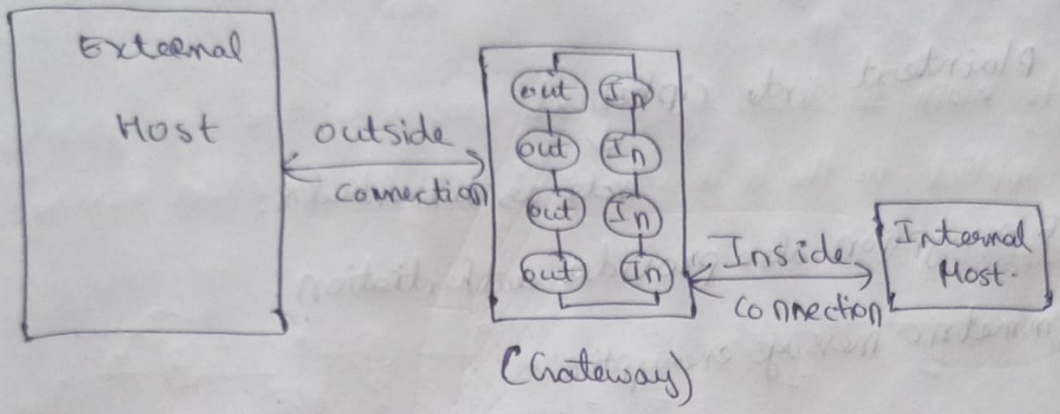
Disadvantage:-

1 processing overhead -

Circuit-level Gateway:-



1. It uses 2 TCP connections
2. a. B/w Internal host and Gateway.
   b. b/w External host and Gateway.
3. Faster than previous (2) types



4. First Internal Host will send a request to the Gateway
5. Gateway will check for the authentication, if ok, then the request will send to external host.
6. Then, the external host will send a response and sent to Gateway.
7. Again gateway will check for authentication and sends the responses to Internal host.

Advantages of Firewalls:-

1. More secure
2. prevents Hacking.
3. stops spyware.

Disadvantages of Firewalls:-

1. Cost
2. User restriction
3. Performance
4. Complex operations

Virus:-

It is a s/w piece of code written to change the way a computer operates and spread from one pc to another.

Malware can be classified into several categories depending on propagation and concealment

Malware is combination of 2 words

Malicious + software = Malware

Propagation

* Virus :- human-assisted propagation.
* Worm :- automatic propagation without human assistance.

Concealment:-

* Rootkit:- modifies operating system to hide its existence.
* Trojan :- provides desirable functionality but hides malicious operation.

Insider Attack:-

* An insider attack is a security breach that is caused (or) facilitated by someone who is the part of the very organization that (controls) builds the asset that should be protected.
* In case of malware, an insider attack refers to security hole that is created in a software system by one of its programmers.

Backdoor:-

* Backdoor is also called sometimes as "trapdoor".
* It is a hidden feature (or) command in a program that allows a user to perform actions he (or) she would not normally be allowed to do.
* when it is used in normal way, the program works completely as expected.
* But if the hidden feature is activated, the program does something unexpected often in violation of security policies.

Non-malicious Backdoors:-

* Some Backdoors are put into programs by it's programmers.
* DeBugging purpose (to skip some heavy (or) long steps to speed up debugging).
* Many computer games have backdoors.
  (Secret key code to exchange gaming role)

Malicious Backdoors:

* Deliberate backdoors inserted by malicious programmers.
  * Blackmail, secret previleage.
* Backdoor created by malware on compromised machines
  * opens tcp listening service, anyone can have a shell connection to the machine with out account and password
  * Ex:- Code Red II.

Logic Bombs:-

* A logic Bomb is a program that performs a malicious action as a result of certain logic Condition.
* Example of a logic bomb with a backdoor where a programmer puts in a logic bomb that will crash the program on certain date.

Defenses against Insider Attacks:-

* Avoid single point of failure
* Use code walk throughts.
* limit authority and permissions.
* Cntrol software Installations.

Trojan horses:-

* A trojan (horse) (or) (Trojan) is a malware program that appears to perform some useful task, but which also does something with negative consequences.
* Trojan horses can be installed as a part of payload of other malware but are often installed by users (or) administrators either accidentally (or) deliberately.

Adware

spyware

Signatures:- A malware Countermeasure.

* Scan compare the analyzed object with a database of signatures
* A signature is a virus finger print.

White/Black listing:-

* Maintain database of cryptographic hashes for
  * operating system files.
  * popular applications
  * known infected files.
* Compute hash of each file in hard drives.
* look up into data Base to compare.

Ex:- Trip wire software

Heuristic Analysis:-

* Used to identify new and "zero day" malware

Code analysis:-

* Based on the instructions the antivirus can determine whether (or) not the program is malicious (or) not.
* If the actions are harmful mark as virus.