**Firewalls**

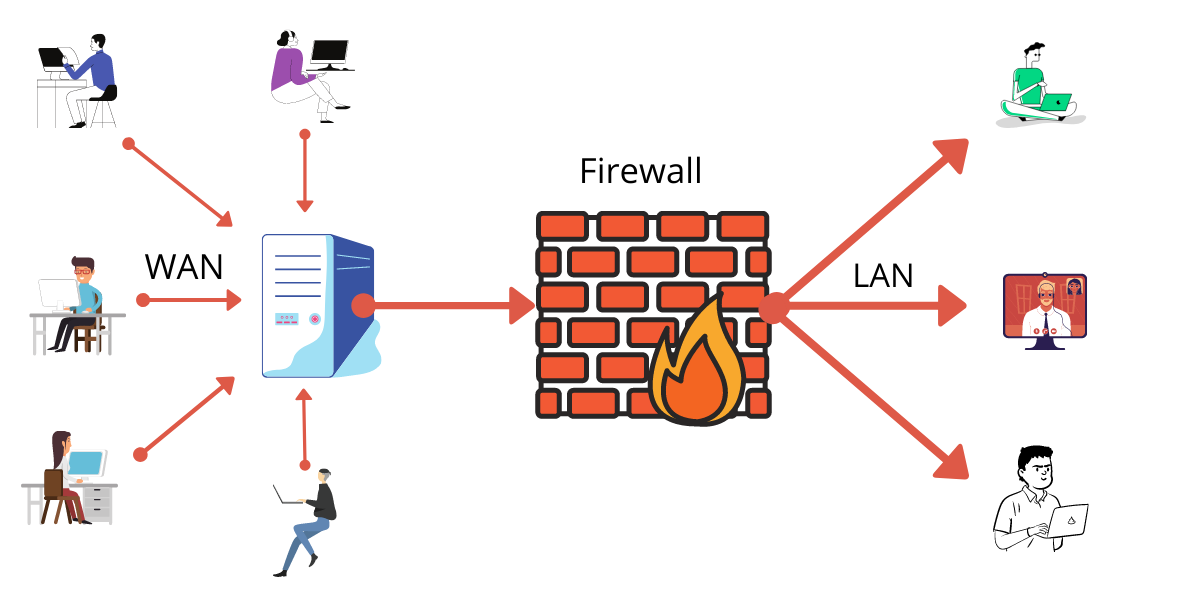
* A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic

Reject : block the traffic but reply with an “unreachable error”

Drop : block the traffic with no reply

* A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



**Characteristics :**

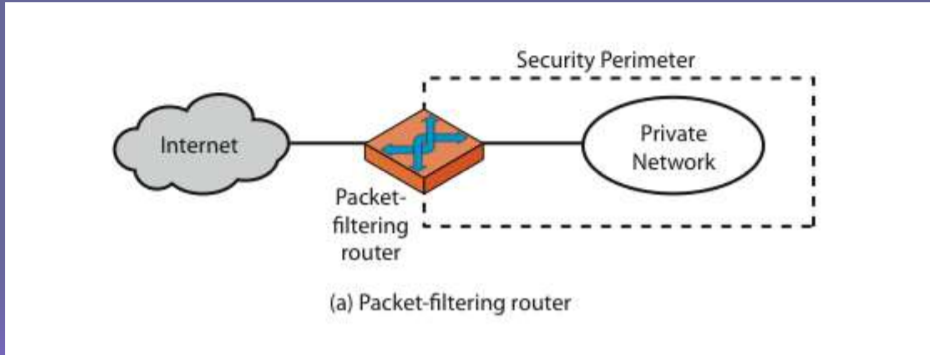
* All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
* Various configurations are possible.
* Various types of firewalls are used, which can be implemented
* various types of security policies.
* Blockage against unauthorized access
* Wireless network (Wi-fi) Protection

**Limitations :**

* The firewall does not protect against internal threats, such as a disgruntled(angry) employee or an employee who unwittingly cooperates with an external attacker.
* cannot protect against transfer of all virus infected programs or files
* cannot protect from attacks bypassing it

**Firewalls – Packet Filters**

* It works in the network layer of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.
* simplest, fastest firewall component
* examine each IP packet (no context) and permit or deny according to rules
* hence restrict access to services (ports)
* Packet filtering is also known as static filtering.

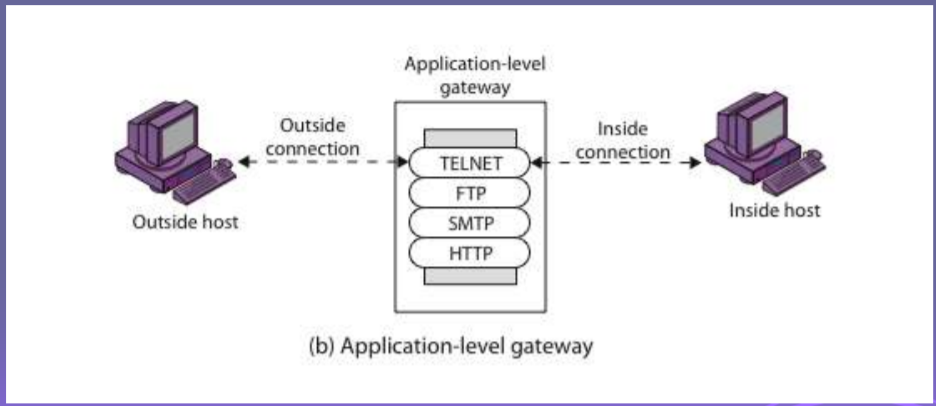


Attacks on Packet Filters:

* IP address spoofing
  + fake source address to be trusted
  + add filters on router to block
* source routing attacks
  + attacker sets a route other than default
  + block source routed packets

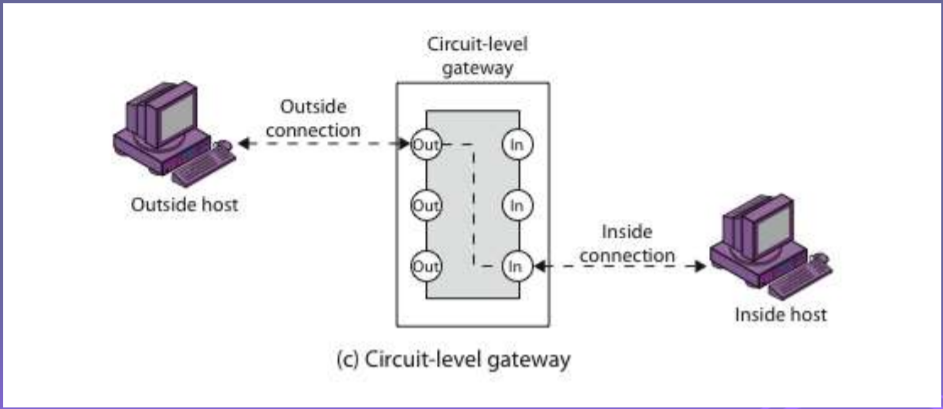
**Firewalls - Application Level Gateway (or Proxy)**

* It operates at the application level. Multiple application gateways can run on the same host but each gateway is a separate server with its own processes.
* provide the most secure type of data connection.
* has full access to protocol
  + user requests service from proxy
  + proxy validates request as legal
  + then actions request and returns result to user
  + can log / audit traffic at application level
* need separate proxies for each service

****

**Firewalls - Circuit Level Gateway**

* **Generally, these circuit-level gateways work at the session layer of the OSI model.**
* To determine whether the session request is confirmed or not by the circuit-level gateway is with the help of handshaking between packets.
* SOCKS is commonly used
* relays two TCP connections

****

**Viruses**

* A virus is a fragment of code embedded in a legitimate program. Viruses are self-replicating and are designed to infect other programs. They can cause system crash, destroy files. On reaching the target machine a virus dropper (usually a trojan horse) inserts the virus into the system.
* **File Virus:**
  + This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called a Parasitic virus because it leaves no file intact but also leaves the host functional.
* **Macro Virus:**
  + macro code attached to some data file
  + Unlike most viruses which are written in a low-level language (like C or assembly language), these are written in a high-level language like Visual Basic. code is now platform independent.
* **Email Virus:**
  + spread using email with attachment containing a macro virus
  + triggered when user opens attachment
  + or worse even when mail viewed by using scripting features in mail agent
  + hence propagate very quickly
  + usually targeted at Microsoft Outlook mail agent & Word/Excel documents
  + need better O/S & application security

**Intrusion Detection System (IDS)**

* An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.
* Two types :
  + **Statistical anomaly detection**
  + **Rule-based detection**

**Statistical Anamoly Detection:**

* It studies the behaviour of the user over a period of time. Based on the data that is processed we make certain rules which are used in future to prevent the intrustion.
* Rules are created to differentiate between legitimate user & illegal user
* Two types:
  + Threshold Detection
  + Profile based detection
* Threshold Detection:
  + This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
  + For Example : if X person uses facebook for 2 hours everyday, if a hacker uses X person’s credentials and uses facebook for more than 2 hours i.e, more than the threshold limit
  + Certain threshold are defined to each user if threshold is crossed then it is considered as intrusion
* Profile Based Detection
  + A profile of the activity of each user is developed and used to detect changes in the behaviour of individual accounts.
  + For Example : if X person uses sites which are related to educational content, then if the attacker uses X person who accesses movies, torrents, etc.
  + There is a certain shift of users behaviour.
  + Profiles are created for each user if they are matched for any illegal activity

**Rule Based Detection:**

* In rule-based detection we make certain rules i.e, rules are defined and if a particular user breaks the rules then it marks that user as intruder
* Anamoly Detection:
  + Rules are developed to detect deviation from previous usage patterns.
* Penetration Identification:
  + These are Expert intelligent systems that tries the user is sending/receiving packets & from that analysis the legitimate and illegal users are classified