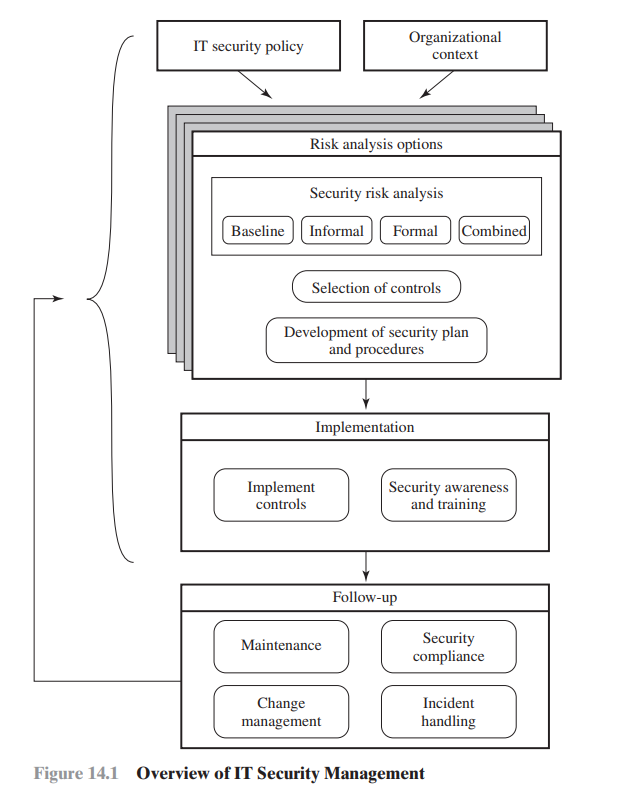
---------------------------------------------------------Chapter # 14 starts ---------------------------------------------------

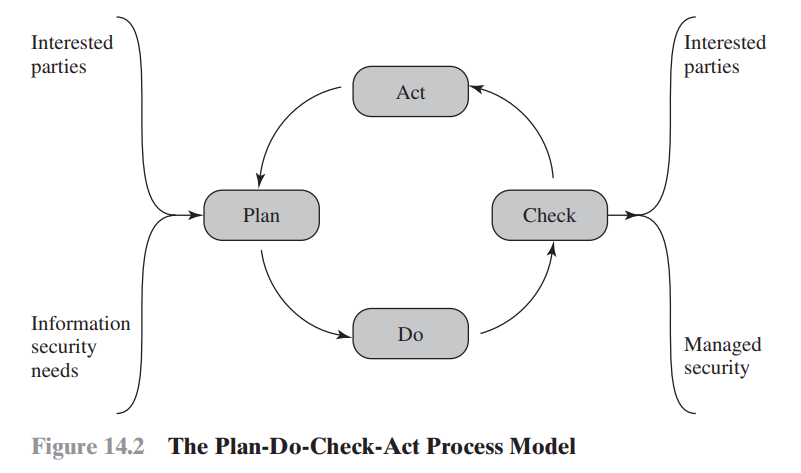
Organization need **an IT security officer**/staff because of:

* Consistent overall supervision
* Interact with senior management
* Maintain security, plans, and policies
* Handle incidents
* IT security and training programs

**Security Risk Assessment techniques:**

1. **Baseline Approach**: basic general level of security controls on systems using baseline documents, codes of practice, and industry best practice. goal is to implement generally agreed controls to provide protection against the most common threats.  
   Recommended for small size organisations that are secured at base level  
   +) doesn’t require additional resources because we have baseline docs  
   +) can be replicated to large systems  
   -) variations in risks are not considered  
   -) baseline may be too high, resulting expensive measure, or too low, leaving insufficient security and vulnerable organisation
2. **Informal approach**: expert judgements and fixes by experts and analysts.   
   Recommended for small-mid sized organisations  
   +) Relatively quicker and cheaper.   
   +) Individuals can assess risk unidentified by baseline.  
   -) some risks may not be considered potential. OR incorrect assessment  
   -) differences in results of analysts  
   -) chances of organisation left vulnerable
3. **Detailed Risk / Formal Analysis**: most comprehensive approach including proper implementation of certain steps including identification of assets and threats, vulnerabilities, likelihood, risks, actions and consequences.   
   Recommended for Large organisations  
   +) most detailed examination of risks   
   -) very costly and time taking
4. **Combined approach**: initially baseline, informal analysis to identify threads, formal assessment on threats & iterated over time.  
   Recommended for most organisations  
   +) better use of time & money  
   -) might miss some risky alerts





---------------------------------------------------------Chapter # 14 ends ----------------------------------------------------

---------------------------------------------------------Chapter # 19 starts ---------------------------------------------------

Computer crime, or cybercrime is a crime in which computers or networks are the tools and targets of the activities

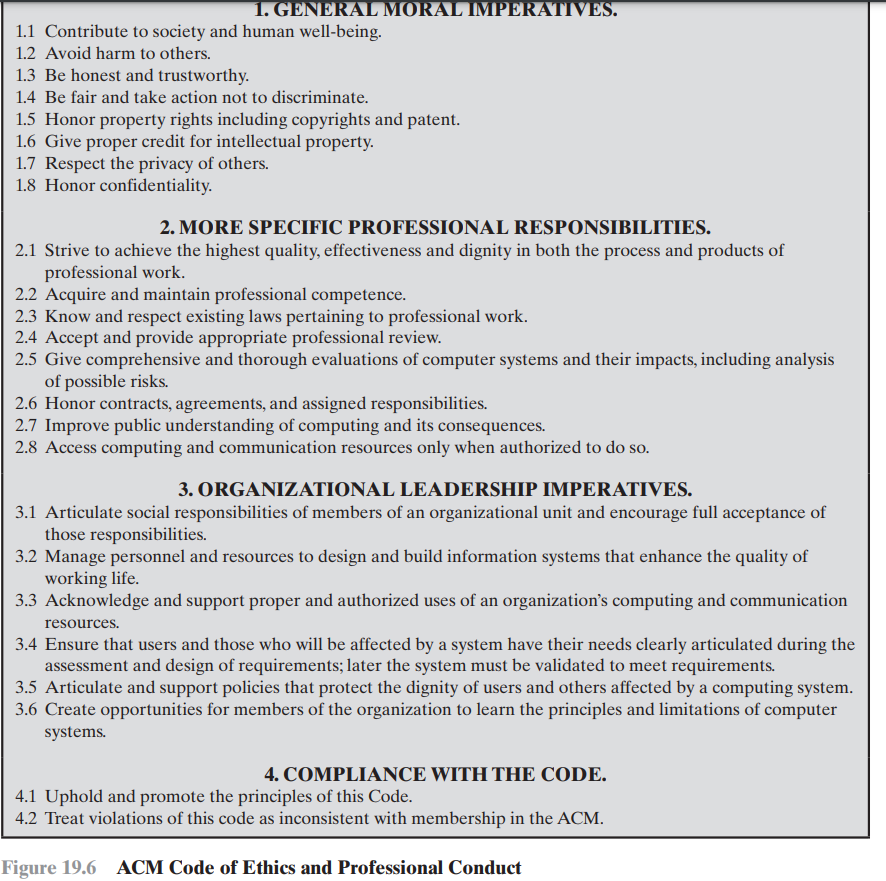
**Types of Computer crimes:**

1. Computer **as targets**: to acquire iformation or unauthorized access gain attacking CIA of data and system privacy.
2. Computer as **storage devices**: computers can be used to get stored password or crack vaults
3. Computer as a **communication tool**: to deal illegaly like selling drugs, gamblings, fraud or pornography

**PECA:**

1. Copying ot transferring data
2. Create a sense of panic, fear and insecurity
3. Unautorized access of gain
4. Issueance of SIM (dhokay se)
5. Dignity of person, harm his/her reputation
6. Modesty/expose his pictures
7. Child pornography
8. Cyber stalking
9. Spamming

**ACM:**



**Law enforcement** inversely relates with success of criminals, due to:

* Lack of investigator’s knowledge
* Required technology >>>>> budget
* Global nature of criminal
* Lack of interaction with legal or law enforcing agencies
* Agencies are corruopt themselves

Cybercriminals **identification challenges**:

* Lack of investigatrors knowledge
* Difficult to profile
* Young, underage or overage
* No epic behavior
* No database exist for identifying criminals

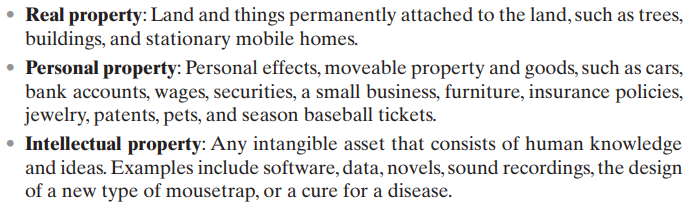
**Victims are affected** by:

* Success of criminals and lack of law enforcement
* Organisations donot invest in security aspects
* Reporting rates tends to be low

Management needs to:

* Understand the case
* Understand inputs and process the solutiions and processings

Intellectual property:

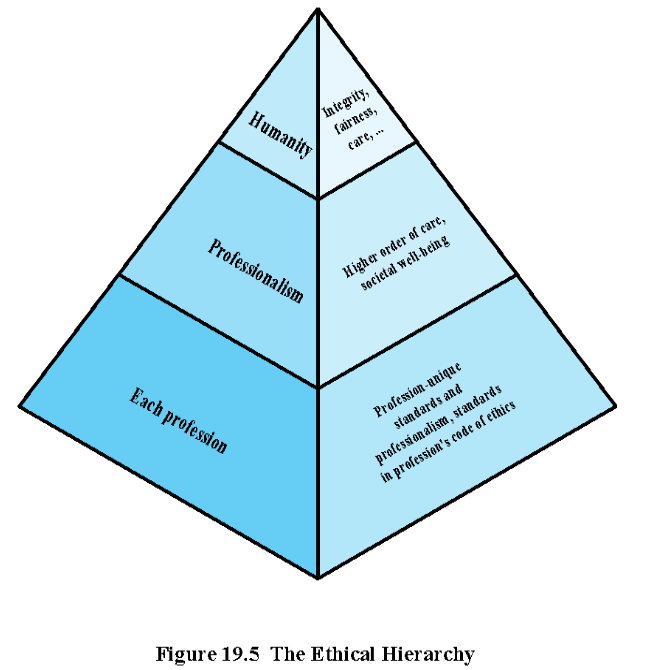


**EU(1998):** ensure to protect Fundamental rights of privacy while processing information

Member states can have flow information within the EU

* Organizations must notify individuals what personal information they are collecting
* Consent of individuals related to 5Ws of data
* Organization uses data only for good cause
* Individuals can CRUD their personal info anytime
* Third parties must secure the data as second party does
* Organization must have legal law enforcement agencies with them

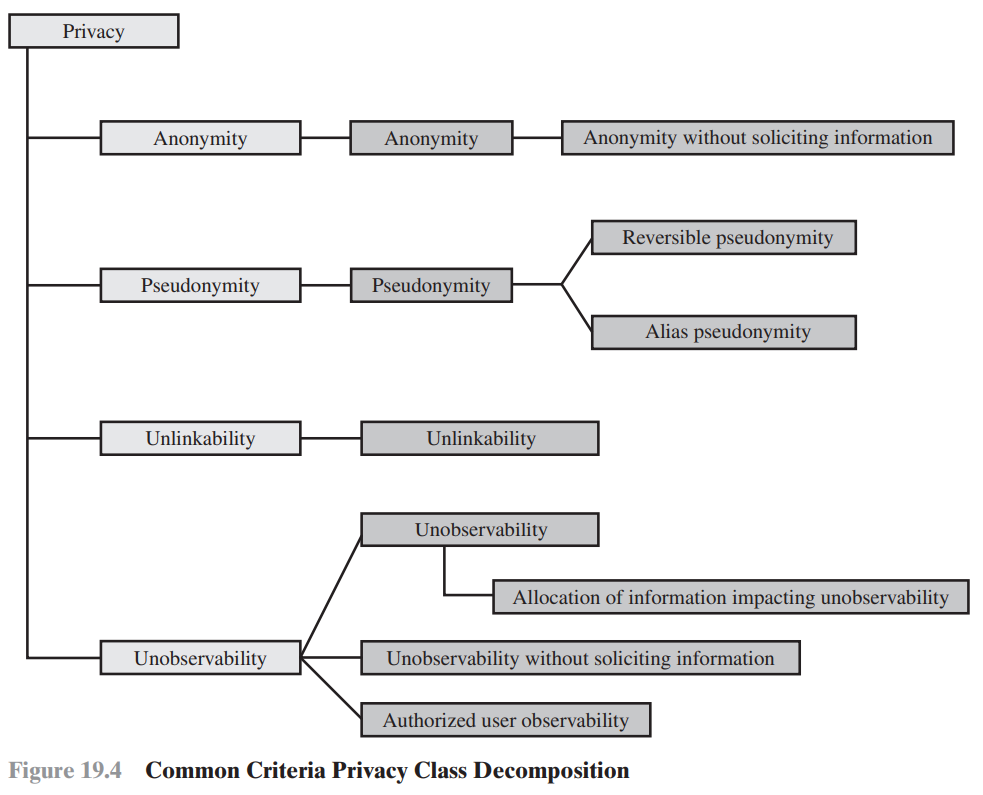
Ethics: A system of moral principles that relate to benefits and harms of some activity



**Ethical issues from computer** use:

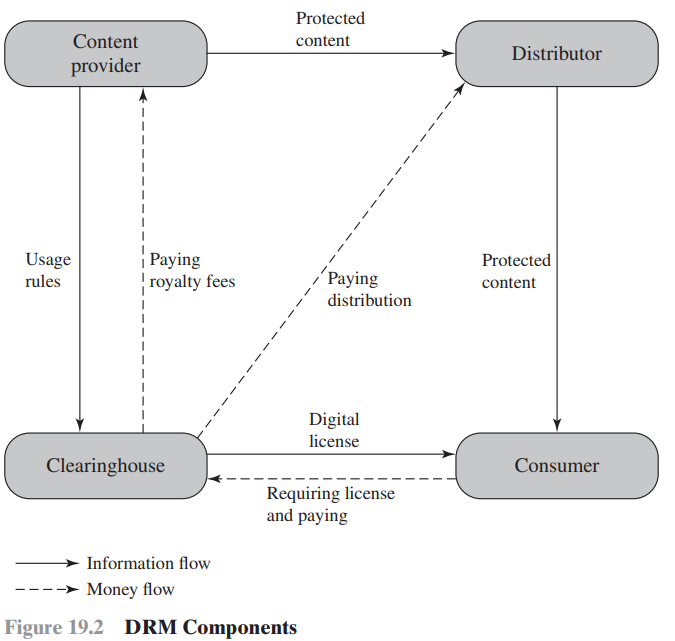
* Repositories and processor of information
* Producers of new assets
* Instruments of acts (service providers and users both are responsible for information)
* Symbol of deception (computers can make mistakes)

Computing **artifacts** are software applications programs for general purpose like robots, phones, Web bots.



**Privacy decomposition** 4 criterias:

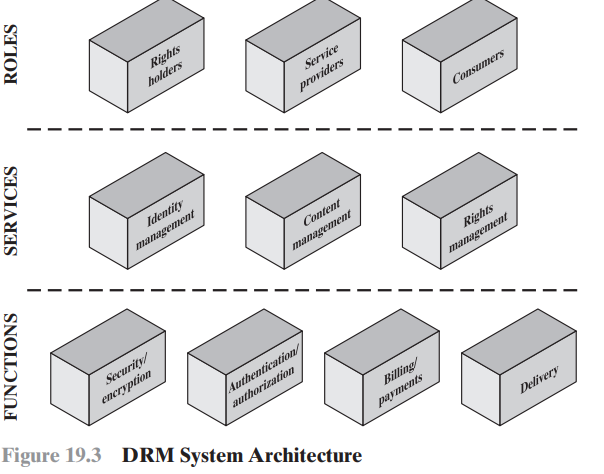
1. **Anonimity**: ensures that a user can utilize a resource without revealing their identity. linked based on user IDs rather than personal information.
2. **Psedunomity**: system provides an alias to prevent others from determining the user's identity
3. **Unlikeability**: unshared resources usage of user. emphasizes separating activities of user to prevent correlation.
4. **Unobservability**: Users can use a resource or service without being observed by others, especially third parties. cannot determine whether an operation is being performed



**DRM** is system of tools to protect intellectual property management & digital content. Its objectives:

Content protection, variety, compatibility, & distributions.

1. **Content provider**: data bhejne wala jese Spotify
2. **Distributor**: data lene wala jese outfitters
3. **Consumer**: hum
4. **Clearing house**: transactions manage krne wala jese paypal.



---------------------------------------------------------Chapter # 19 ends ---------------------------------------------------

---------------------------------------------------------Chapter # 08 starts ---------------------------------------------------

Intruders – Cyber Criminals, can attack on

* Personal identity
* Financial credentials
* Corporate info
* Data theft and ransoming, a software which encrypts all the files and computer systems

Classes of **intruders**:

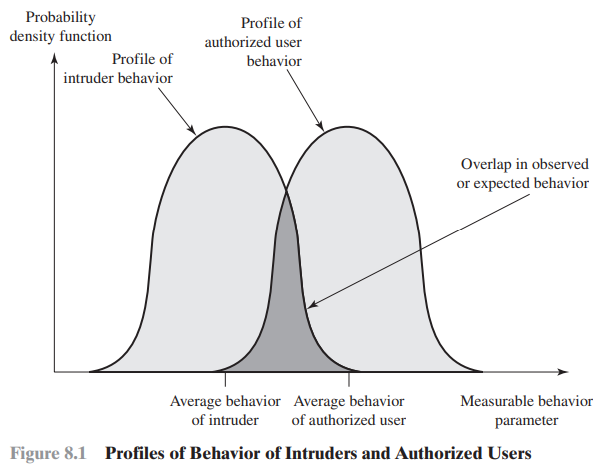
1. **Activists**: internal/external individuals influenced by socio/political causes
2. **State Sponsored**: group of hackers sponsored by government to harm something.
3. **Others**: different than above. Inspired by technical challenges

Intruders **Skill level:**

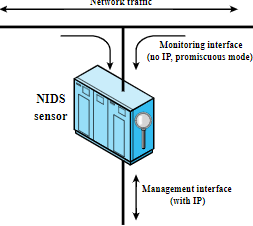
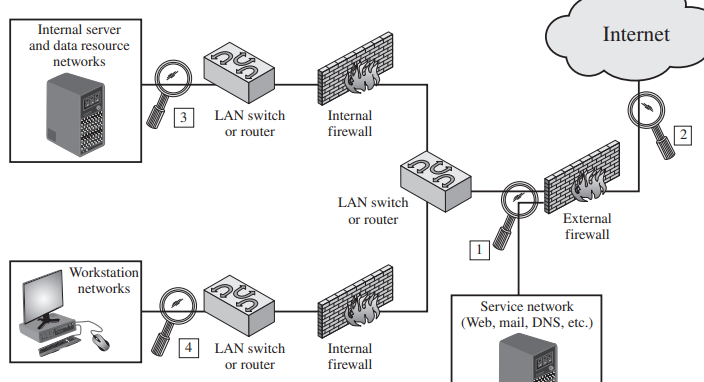
1. **Apprentice**: least skilled hackers. Easy to defend. Script-kiddies coz they use scripts to attack
2. **Journeyman**: with sufficient technical skills to use or extend tools
3. **Master**: high level technical skilled hacker

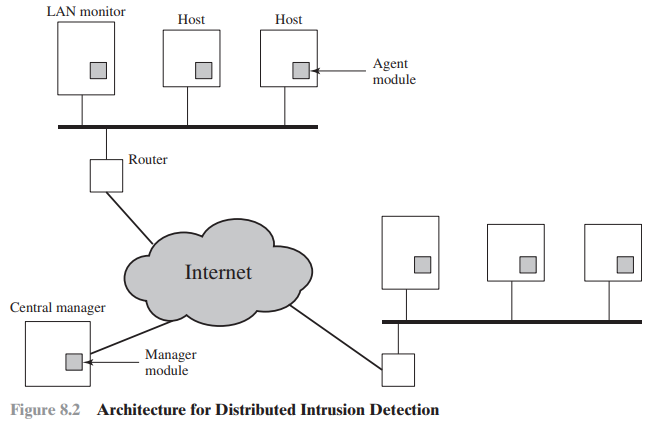
**Steps** included in intrusioning:

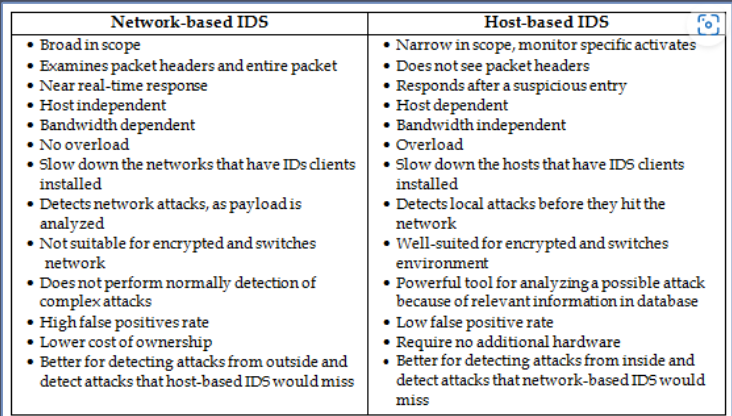
* **Target acquisition**: find websites
* **Initial access**: Brute-force, guessing, NcR, NpR
* **Privileges**: Identify and exploit vulnerability
* **Information gathering**: scan and transfer files to external repos
* **Maintain access**: Install a remote system for accessing through backdoor
* **Cover tracks**: hide installed files. Delete logs



Intrusion Detection Systems **(IDS):** identify suspicious activities

1. **Host based (HIDS)**: monitors characterstics of host and systems. Adds a security layer. Can use either of analysis approach.   
   Data sources: systems calls, log files, file checksums, access controls
2. **Network based (NIDS)**: monitors and analyzes networks and routes and protocols  
   -> stand-alone **INLINE** sensor, performs intrusion detection and prevention both.  
   -> **passive** sensor monitors a copy of network traffic but not actual. Better w.r.t traffic flow  
   **Passive are more used** because:  
   **low network impact, negligible risk of false-positives, scalability, and flexibility**  
     
    PASSIVE SENSOR DIAGRAM  
   Sensor deployement
3. **Distributed or hybrid**: combination. Normally collects data from sensors. Can analyze input/output behavior





Analysis Approach:

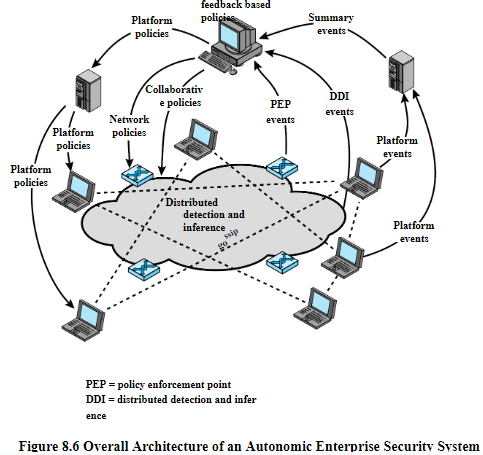
1. Anomaly detection: (Statistical, knowledge based uses past records to judge, AI or ML)   
   collection of data relates to user behavior over time  
   user is verified based on current bahavior of user
2. Signature or heuristic detection: (observe events – apply rules – decide)   
   known data patterns relate to current behavior  
   only identify known attacks due to known patterns

Detection techniques:

|  |  |
| --- | --- |
| Signature Approach | Anomaly Approach |
| Application layer attack, FTP, HTTP | DOS attack |
| Transport, TCP, and network layer attack, IPv4 | Scanning, send traffic and learn from responses |
| Policy violations, use forbidden protocols. | worms |

Stateful Protocol Analysis (SPA) (analysis of protocol states) is a subset of Anomaly approach (General, VAST). Anomoly learns on data and models while SPA used predefined info given by vendors. SPA uses high resources due to Packets inspection, State tracking, complex, large datasets, computes False-positives.

Logging of Alerts: maintaining alerts register. Includes time, connection ID, event type, ratings, protocol, source and destination, ports, bytes transferred, state info i.e username



8.6 not clear………………….. dubara samjho kisi se ………………………………………………………… LEFT LEFT LEFT

---------------------------------------------------------- CHAPTER – 8 ends --------------------------------------------------

---------------------------------------------------------- CHAPTER – 9 Starts-------------------------------------------------

Firewalls are effective to protect LANs. Inserted between LANs and Internet. Protection from IP spoofing and routing attacks

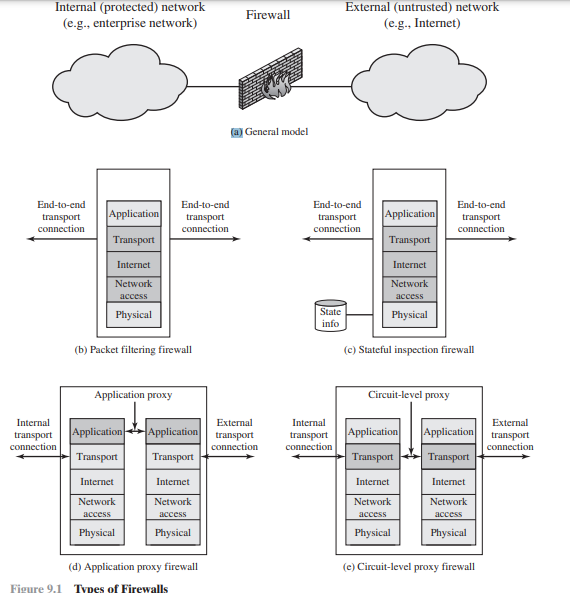
firewall cannot protect against attacks that bypass the firewall i.e. direct connection to organisation that bypass firewall. e firewall may not protect fully against internal threats

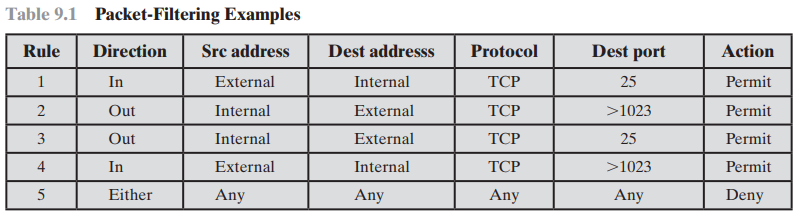
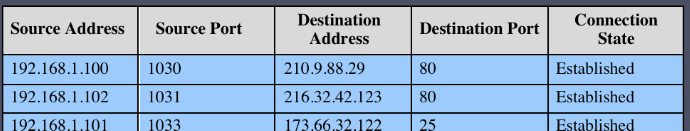
Design Goals:

All traffic must pass through it. Only authorized traffic will pass. It is immune to penetration

Firewall filter characterstics: (Control accesses)

* IP address and protocols: limit access to specific services
* Applciaiton protocol: exchange of info w.r.t protocols like emails going in SPAM. HTTP request goes to authorized sites only
* User identity: secure user identity using IPsec
* Network activity: conditions such as from 9-6 time, rate of requests etc.



1. **Packet filtering:**denies or passes incoming/outgoing packets based on rules. Can’t determine application specific issues. Less secure because only header checked, not data. Limited log book.  
     
   
2. **Statefull inspection** firewall: same as packet filtering but also maintains Connection column  
   
3. **Application level gateway**: known as Proxy Server which checks both, Packet headers and data inside it. It has processing overhead. Host and Internet thinks they are direct, but are not coz proxy server in between. Used when focus is on Application layer and data control. Higher security than Circuit as Data is inspected
4. **Circuit level gateway**: same as proxy server but it makes a new connection every time packet comes/goes. Used when focus is to create connections and inspect/control Transport layer data and stuff.