Firewalls

- It is a network software / hardware device.
- All the data passes only through fire-wall.

} Best practice to achieve maximum possible protection

Hard-ware firewall (Appliance Firewall)

↓ physical device

attached bt a computer network and gateway.

Eg: broadband router

software firewall (Host Firewall)

↓ simple program installed on a computer

that works through the port-numbers and other installed software

7 OSI layers

- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer

Application gateway ← (Application Layer, Presentation Layer, Session Layer)

Circuit level gateway

Network Layer } Packet filter

Packet Filtering Firewall

- Basic type of fire-wall
- Acts like a management program which monitors all the network traffic and filters the incoming packets based on the configured security levels.
- designed to block
  - network traffic IP protocols
  - IP address
  - port number

  if the data packets does not match the established rule-set.

Limitation

- It is the fast solution without any resource requirements.
- These fire-walls do not prevent web-based attacks.
- Will not check the payload

Circuit Level Gateways

↳ works at the session-level of the OSI model by verifying UDP connections/ TCP connections and sessions.

↳ Designed to ensure that the established connections are protected.

↳ Implemented as security software / pre-existing firewalls.

↳ Like packet filtering, they do not check for the actual data although they inspect the information abt transactions

↳ Limitation
Data ← malware but follows correct TCP connection it will pass through the gateway

↳ These are rarely used as stand-alone firewall typically used in the combination of application layer proxy servic and packet filtering featu

in some dedicated fire-wall applications.

Application Level Gateways [Proxy firewalls]

↳ Intermediate device to filter the incoming packets between NETWORK TRAFFIC SYSTEMS

↳ these firewalls transfers the request from clients pretending to be the original clients on the web-server.

↳ Protects the client's identity and other suspicious informatio keeping the network safe from potential attacks.

↳ Once the connection is established, the proxy firewall inspects the data packets coming from source.

↳ If the content of the incoming data packet is protected, the proxy firewall transfers to the client.

↳ This creates an additional layer of security between the client and many different sources on the

IP Security

IP security
↓
Internet Engineering Task Force (IETF) standard suite of protocols b/t 2 communication points across the IP network and provides

- data integrity
- data authentication
- data confidentiality

*) Also defines the ① encrypted ~~and~~, ② decrypted and ③ authenticated packets.

*) secure key exchange + key management } required protocols are defined.

Protocol requires

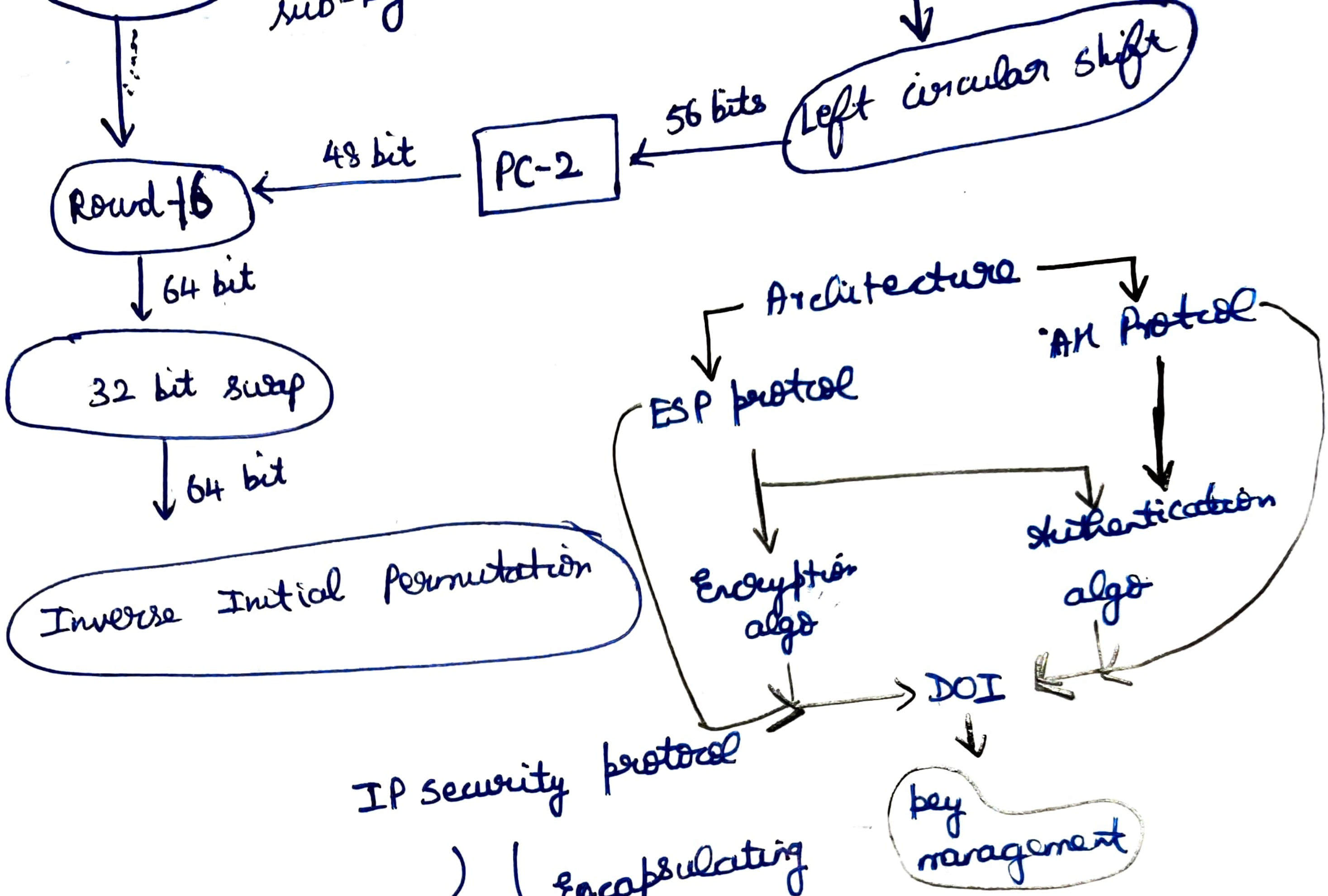
Uses of IP security

- To encrypt the application layer data.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.

*) Router → sending routing data-packets across the public network } provides security

*) Virtual Private Connection

Protects the network data by setting up circuits using IPsec tunnelling in which all the data that is sent between two points is encrypted.



IP security protocol

Authentication Header (AH)

*) Provides mechanism for authentication only.

*) Provides data integrity by using an authentication algorithm.

*) It does not encrypt the packets

Encapsulating Security Payload (ESP)

+) Provides confidentiality only | authentication only | both

*) Protects the packets with an encryption algorithm

*) Provides data-integrity with authentication algorithm.