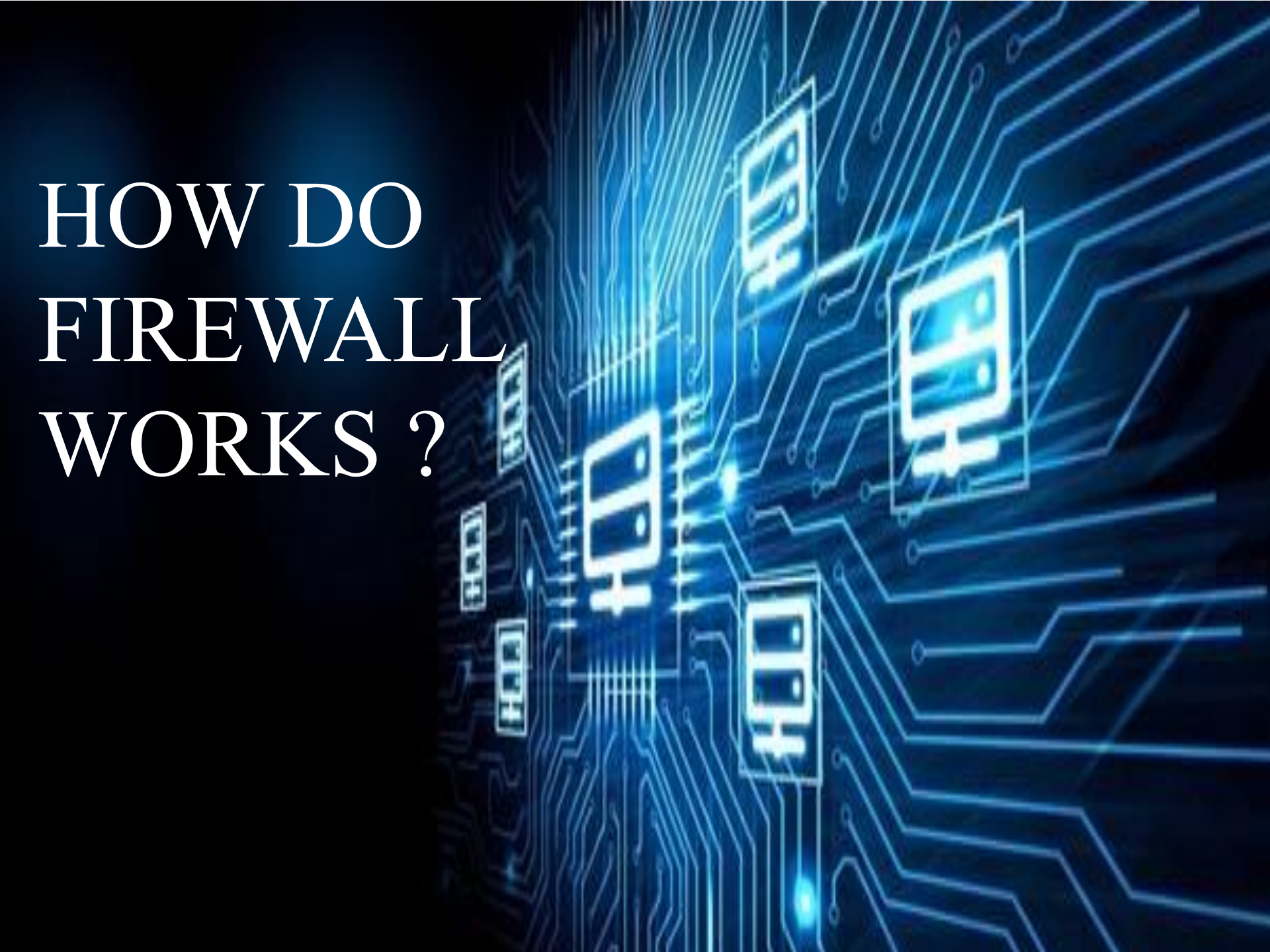
FIREWALL IMPLEMENTATION & ANALYSIS

OUTLINE

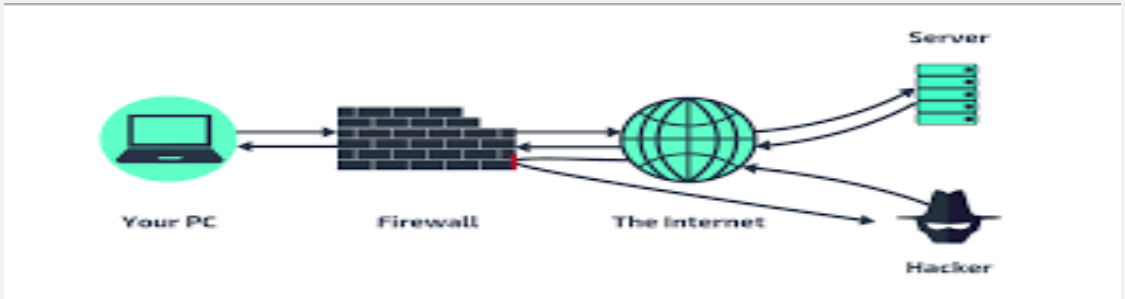
- INTRODUCTION
- FIREWALL DESIGN PRINCIPLES
- FIREWALL CHRACTERISTICS
- WHAT FIREWALLS DO?
- WHAT FIREWALLS CANNOT DO?
- TYPES OF FIREWALLS
- PROS & CONS OF FIREWALLS
- FIREWALL TOOLS
- HARDWARE & SOFTWARE OF FIREWALLS
- REFERENCES

HOW DO FIREWALL WORKS ?



INTRODUCTION

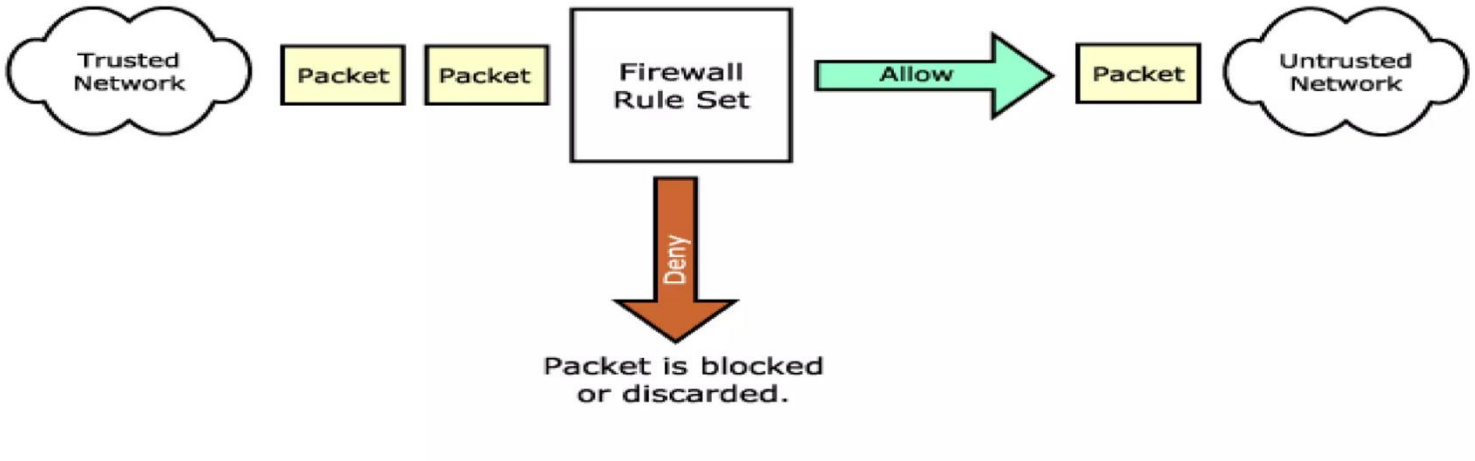
What is a firewall?



- An approach to security
- A system to control access to or from a protected or private network
- Works to implement a security policy defined by an organization
- A private network’s single point of from Internet indruters

FIREWALL DESIGN PRINCIPLES

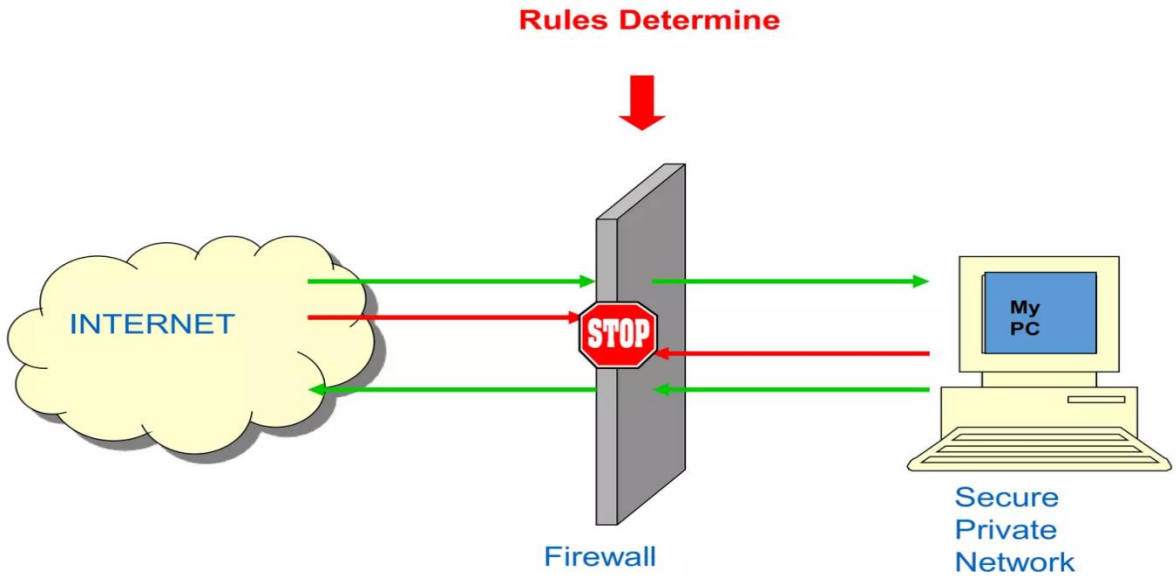
- The firewall is inserted between the premises network and the internet
- AIMS:
  - Establish a controlled link
  - Provide a single choke point
  - Protect the premises network from internet attacks



FIREWALL CHARECTERISTICS

◊*DESIGN GOALS*

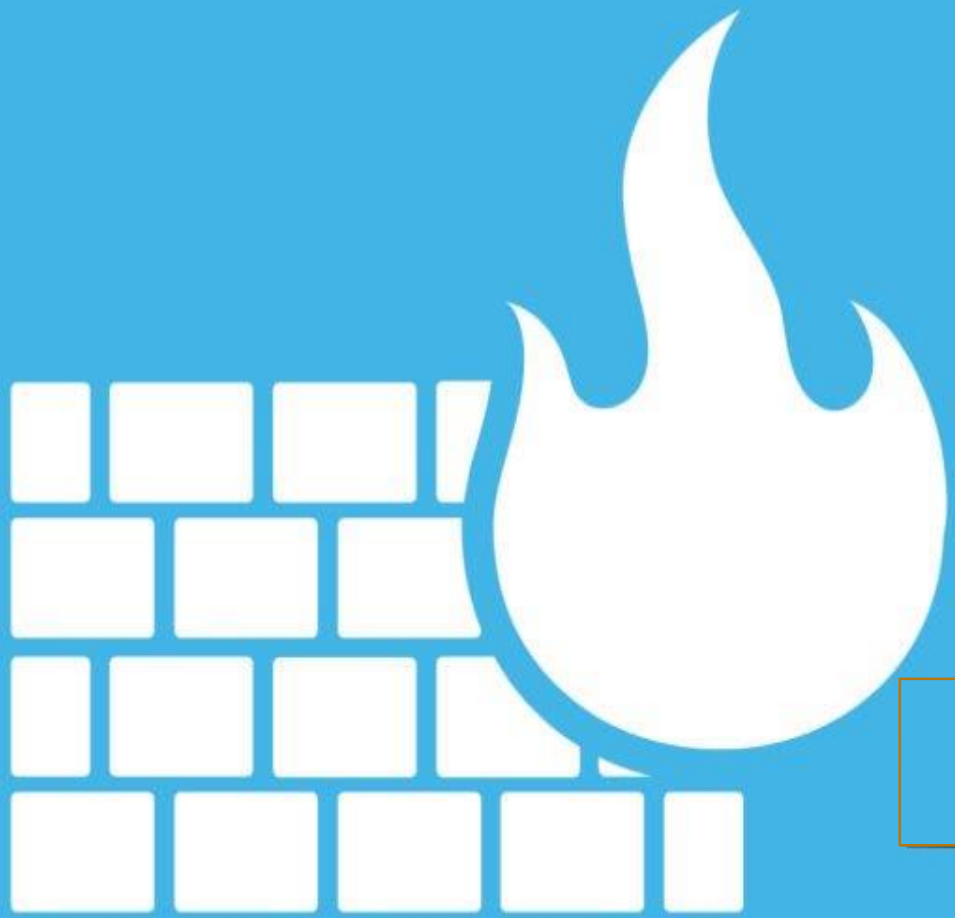
- All traffic from inside to outside must pass through the firewall
- Only authorized traffic will be allowed to pass



FIREWALL CHARECTERISTICS

FOUR GENERAL TECHNIQUES :

1. *SERVICE CONTROL*:
   - Determines the type of internet services that can be accessed
2. *DIRECTION CONTROL*:
   - Determines the direction in which particular service request are allowed to flow
3. *USER CONTROL*:
   - Control access to a service according to which user is attempting to access it.
4. *BEHAVIOUR CONTROL:*
   - Controls how particular service are used.



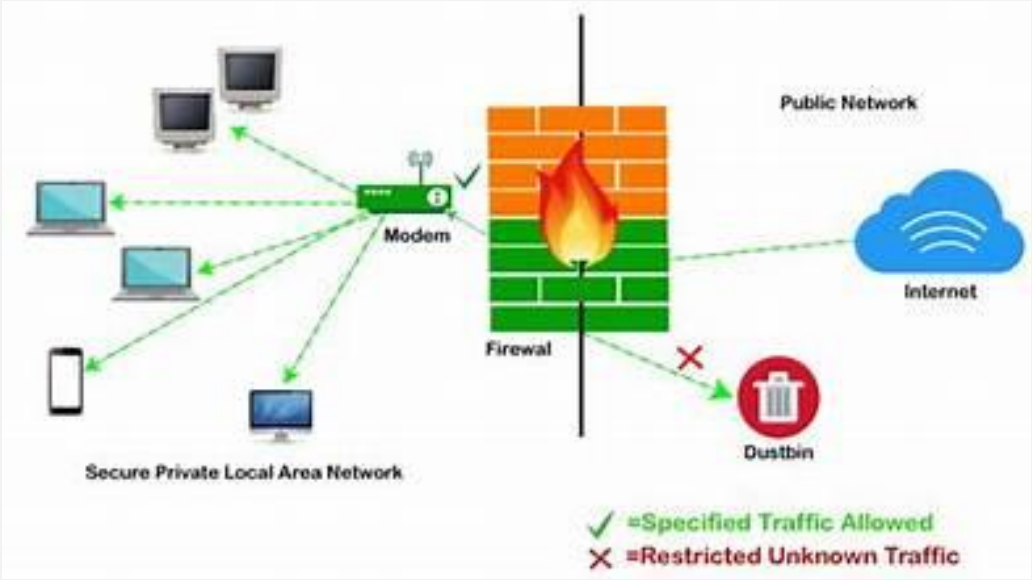
CAN & CAN'T DO !!

FIREWALLS CAN DO..?

- Preventing cyber attacks
- Protecting sensitive data
- Maintaining the privacy and security of computer systems and networks.

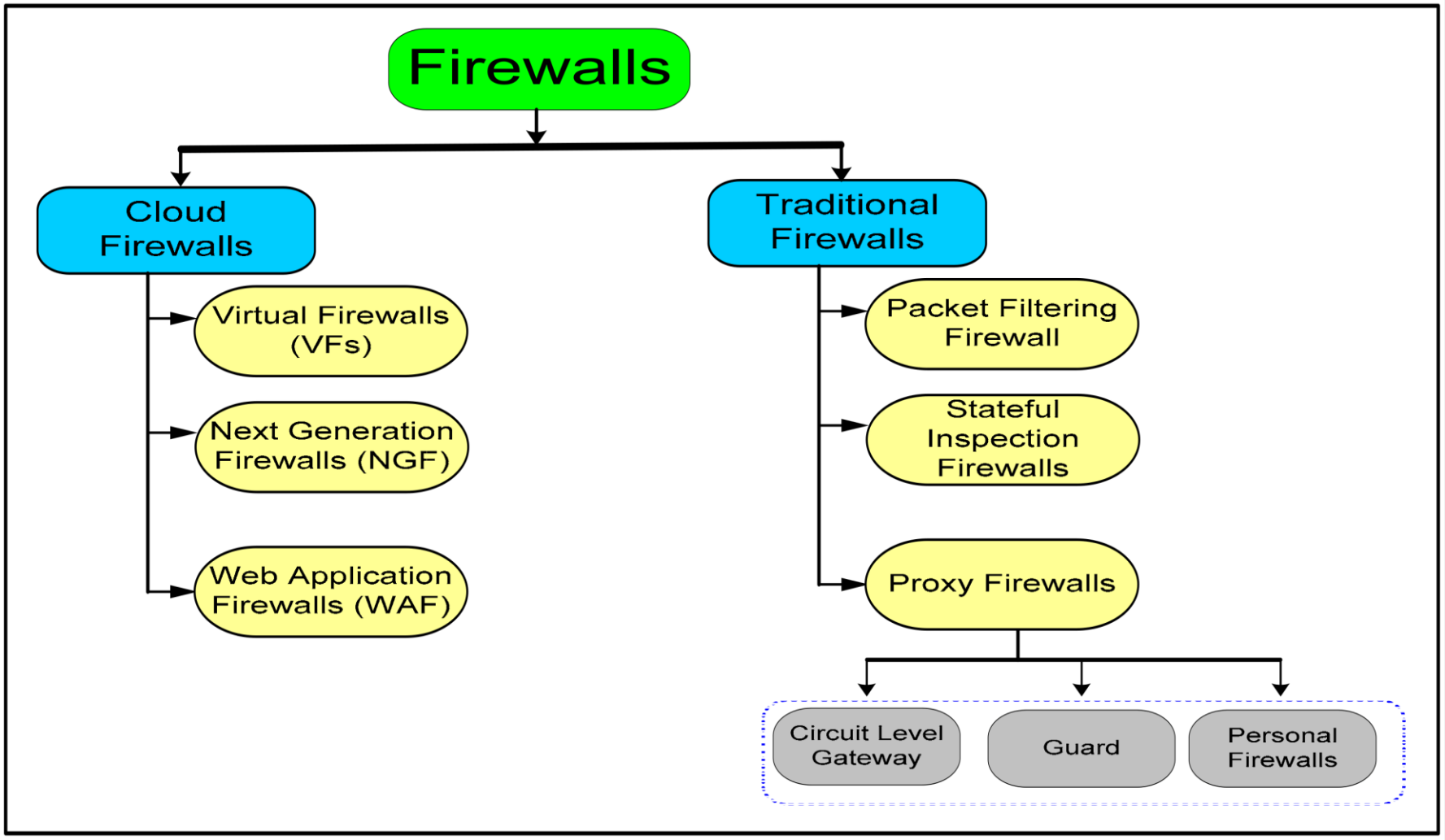
FIREWALLS CAN'T DO..?

- Can't protect you against malicious insiders
- Can't protect you against connections that don't go through it
- Can't protect against completely new threats
- Can't protect against viruses



TYPES OF FIREWALL

Hierarchy flow chart :



Pros & Cons of Firewalls

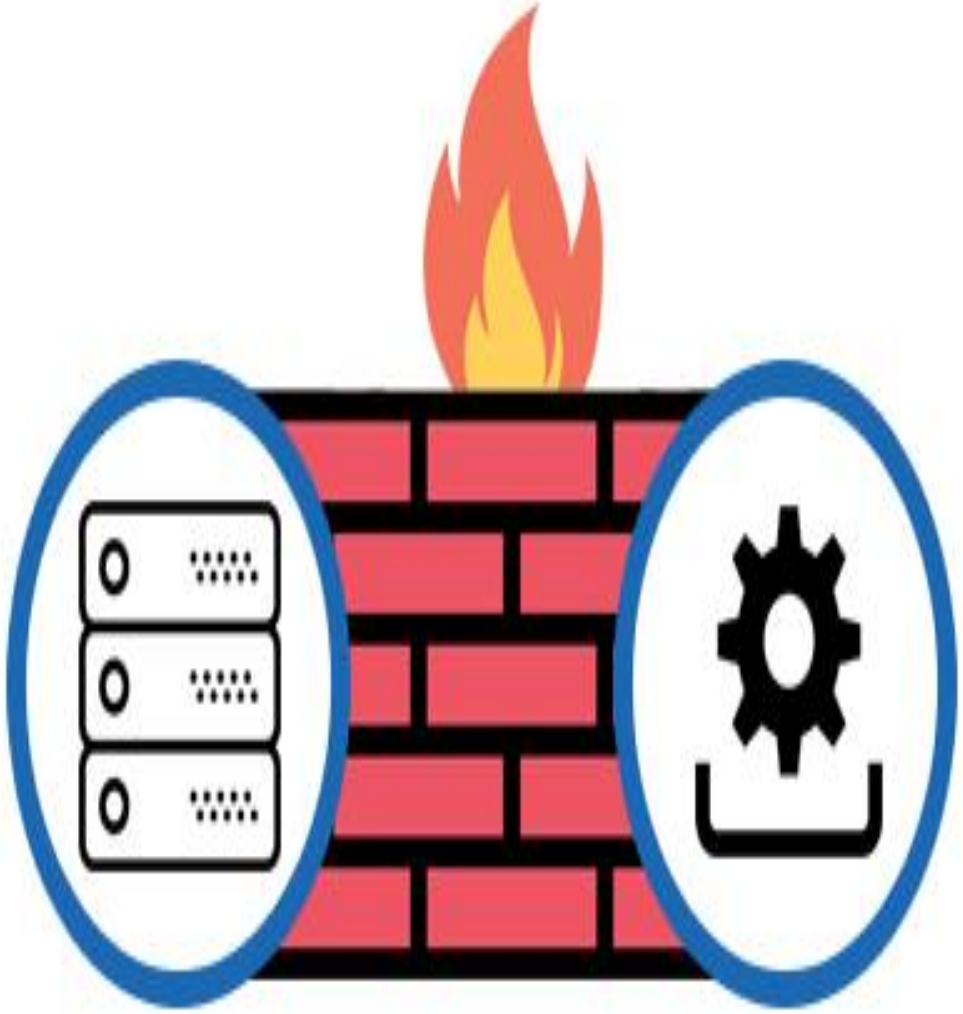
Pros

- Security
- Control
- Privacy
- Performance
- Compliance

Cons

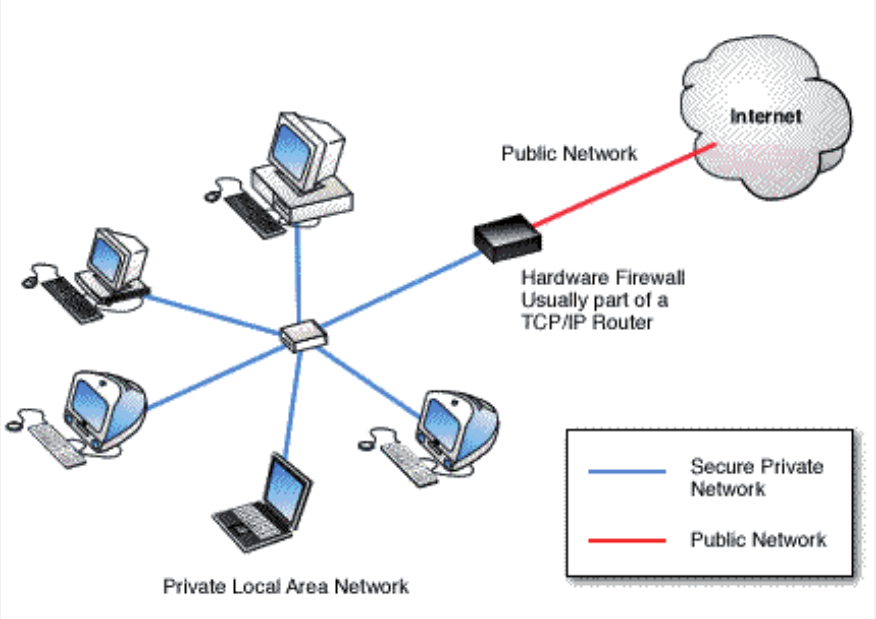
- False sense of security
- Complexity
- Compatibility
- Cost
- Performance

Hardware Firewalls v/s Software Firewalls



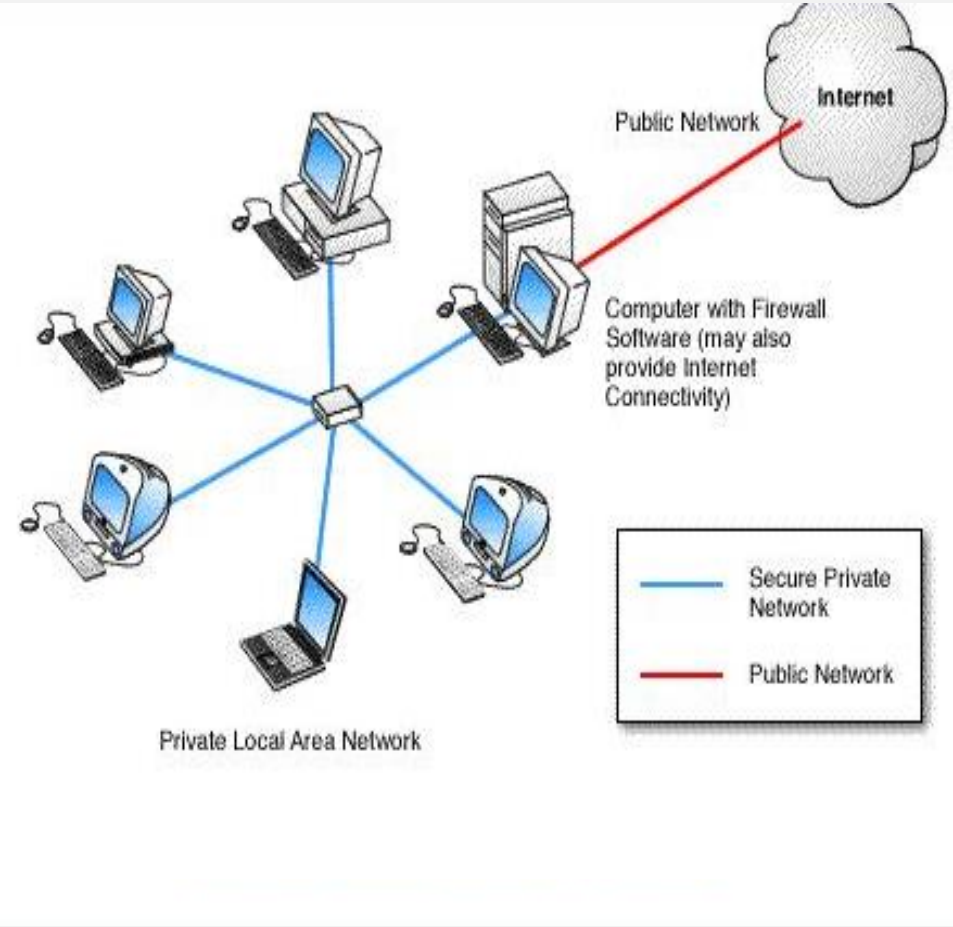
Hardware Firewalls

- Protect an entire network
- Implemented on the router level
- Usually more expensive, harder to configure



Software Firewalls

- Protect a single computer
- Usually less expensive, easier to configure



SOFTWARE FIREWALLS:

The most widely used command-line-based firewall is ***Iptables/Netfilter.***

Some of the frequently used options in iptables are:

- ---append,-A
- ---check,-C
- ---delete,-D
- ---flush,-F
- ---insert,-I
- ---list,-L
- ---new-chain,-N
- ---verbose,-V
- ---delete-chain,-X

REFERENCES :

- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.mdpi.com%2F20763417%2F11%2F19%2F9183&psig=AOvVaw1vJQsN_5QRYZ7SKYWQm6E&ust=1703411596884000&source=images&cd=vfe&opi=89978449&ved=0CBIQjRxqFwoTCJCD0YWlpYMDFQAAAAAdAAAAABAD
- https://www.spiceworks.com/it-security/network-security/articles/what-is-firewall-definition-key-components-best-practices/
- https://www.slideshare.net/ajeetsingh70/firewall-design-and-implementation

THANK YOU

PRESENTATION DESIGN

-S.HARINI
V.SRIMATHI