FIREWALL IMPLEMENTATION & ANALYSIS

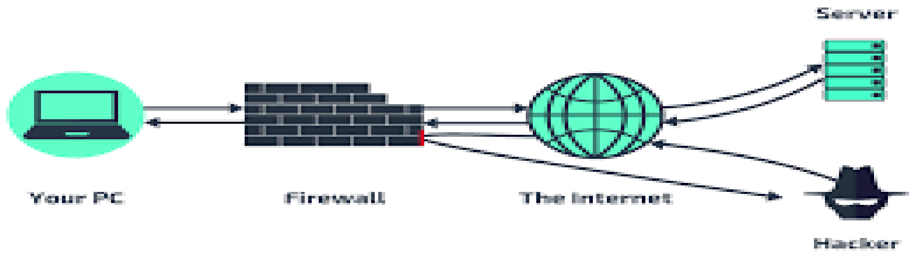
OUTLINE

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

HOW DO FIREWALL WORKS ?

INTRODUCTION

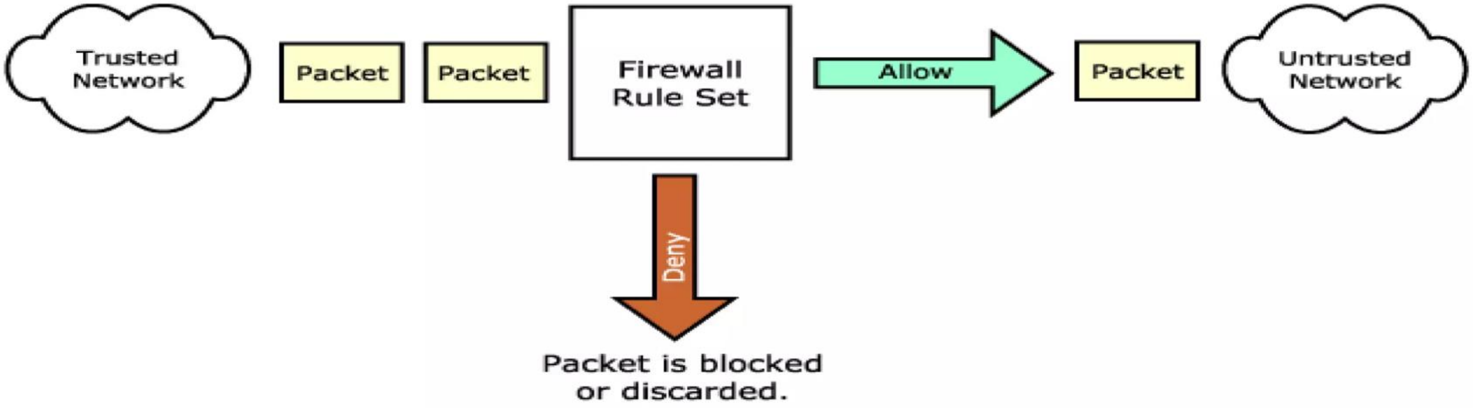
What is a firewall?



- ❖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

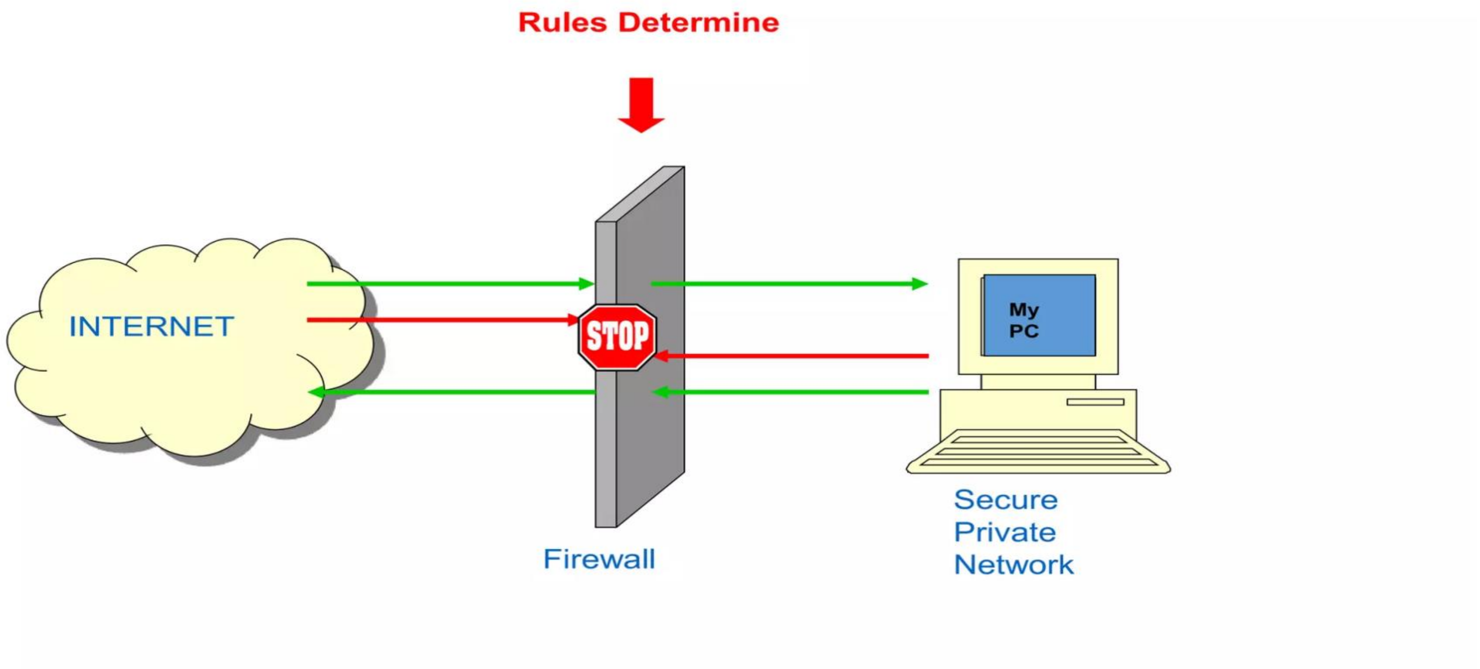
- The firewall is inserted between the premises network and the internet
- AIMS:
  - Establish a controlled link
  - Provide a single choke point
  - Protect the premises network from internet attacks



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*:

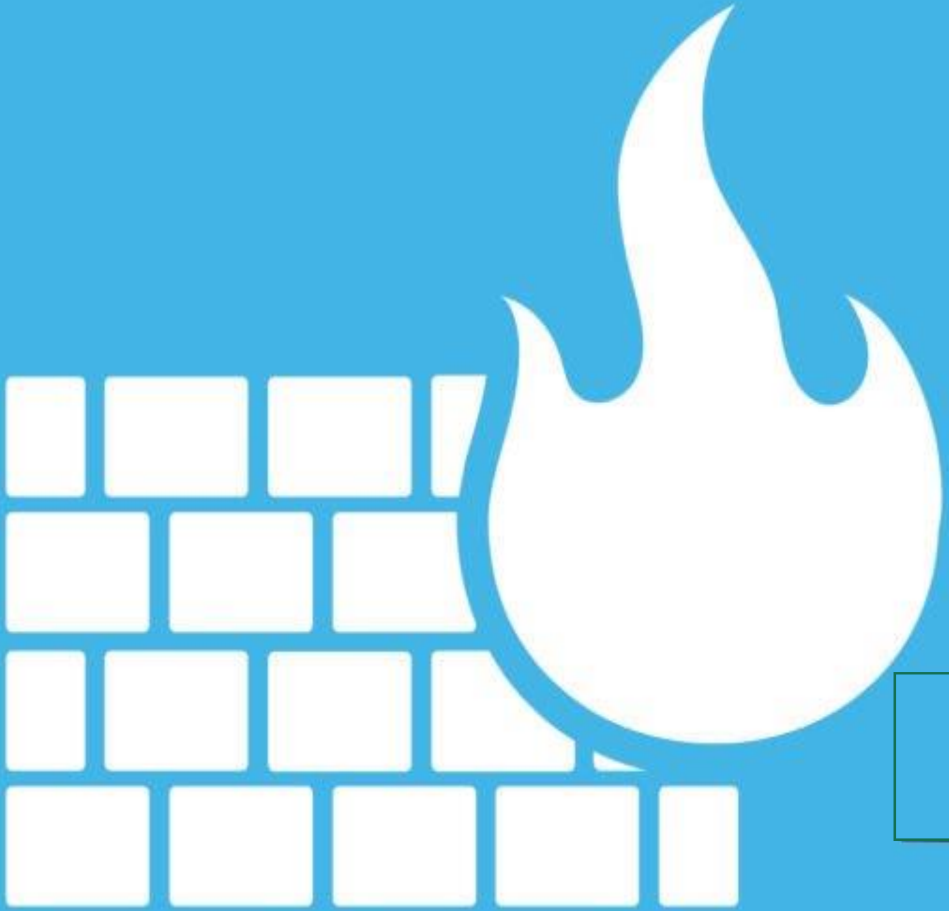
   - Determines the direction in which particular service request are allowed to flow

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.



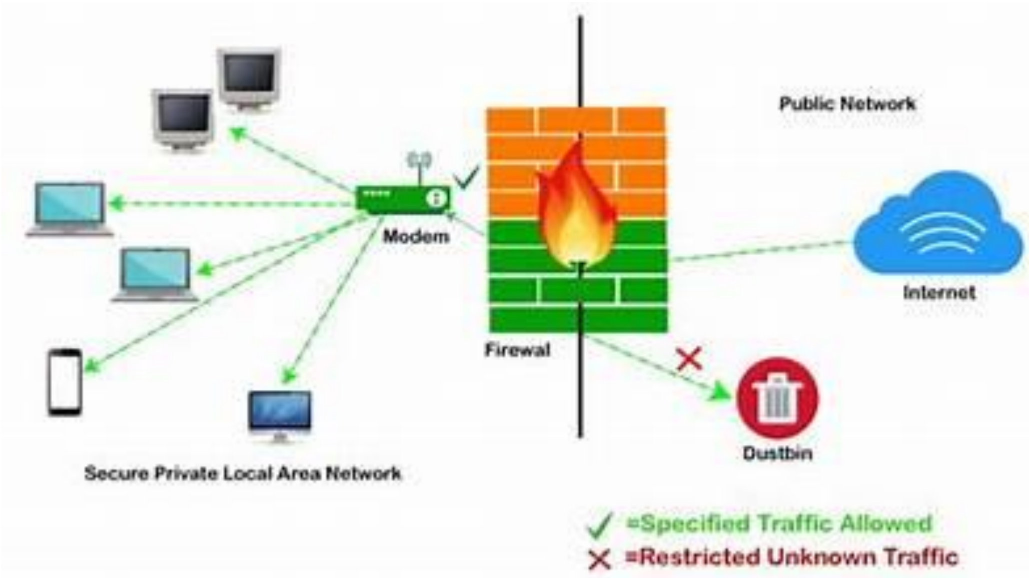
CAN & CAN'T DO !!

FIREWALLS CAN DO..?

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

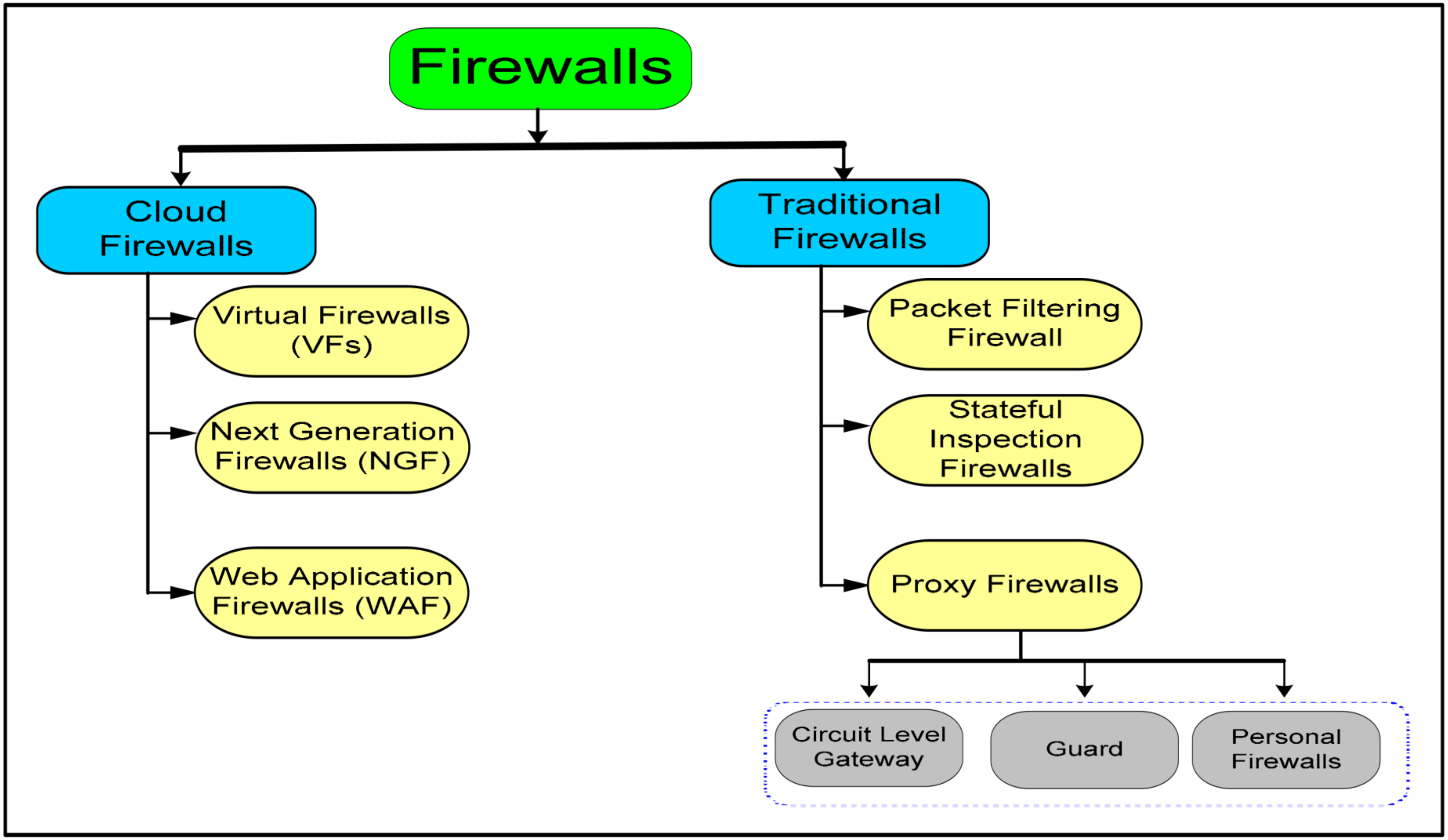
FIREWALLS CAN'T DO..?

- 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


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ =Specified Traffic Allowed
✕ =Restricted Unknown Traffic

TYPES OF FIREWALL

Hierarchy flow chart :



PROS &CONS OF FIREWALLS

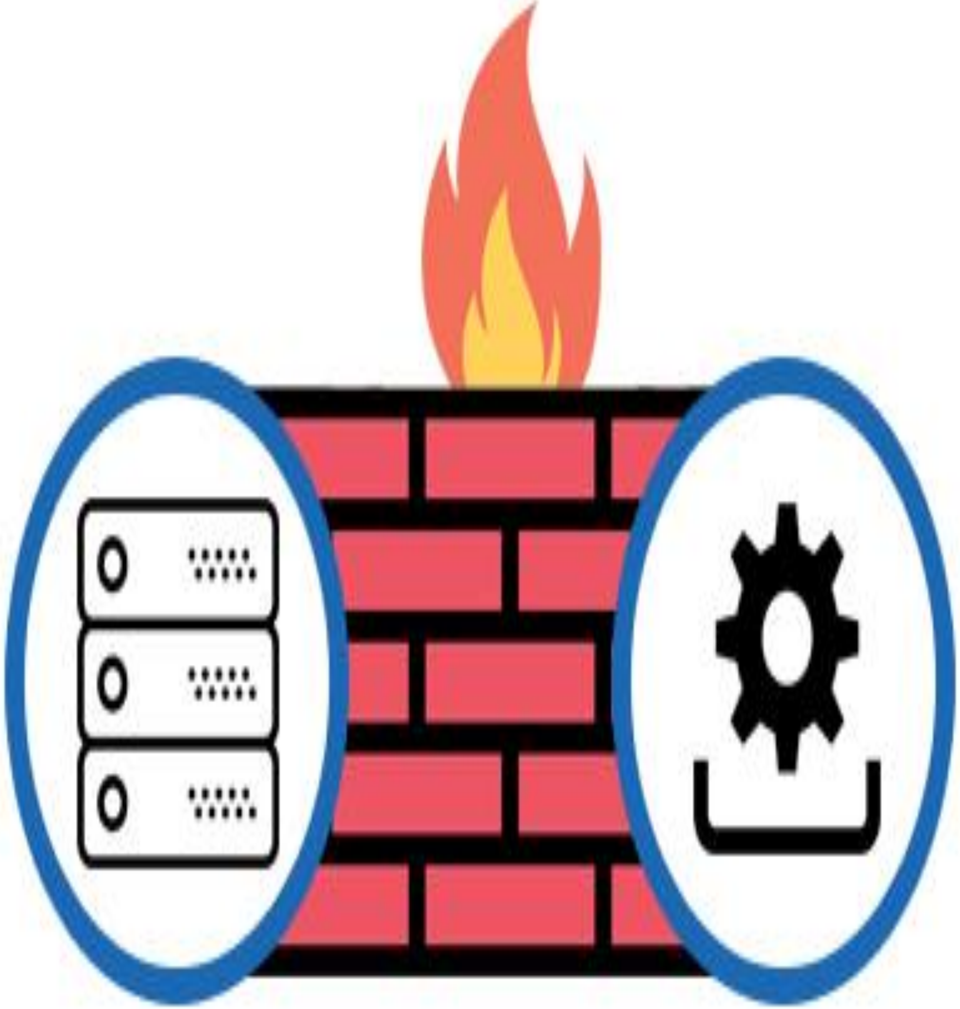
PROS

- Security
- Control
- Privacy
- Performance
- Compliance

CONS

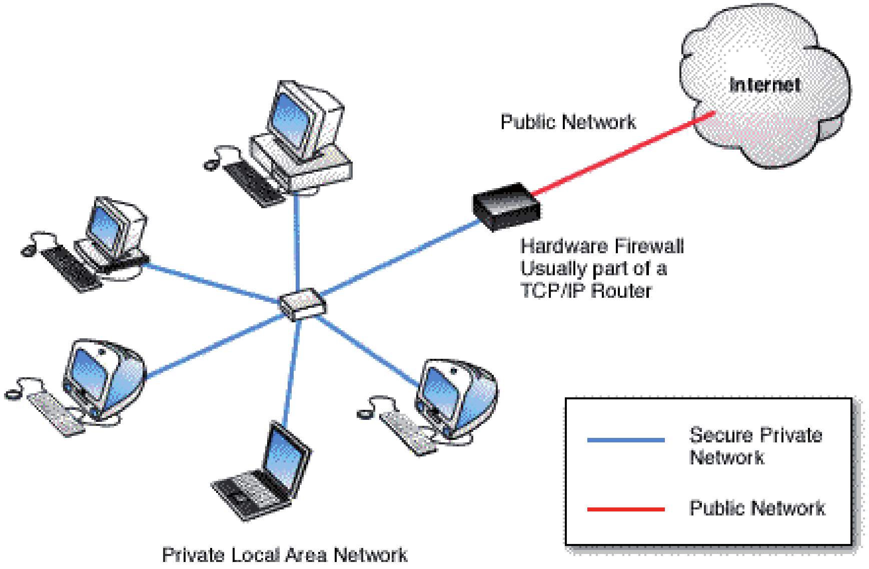
- False sense of security
- Complexity
- Compatibility
- Cost
- Performance

Hardware Firewalls v/s Software Firewalls



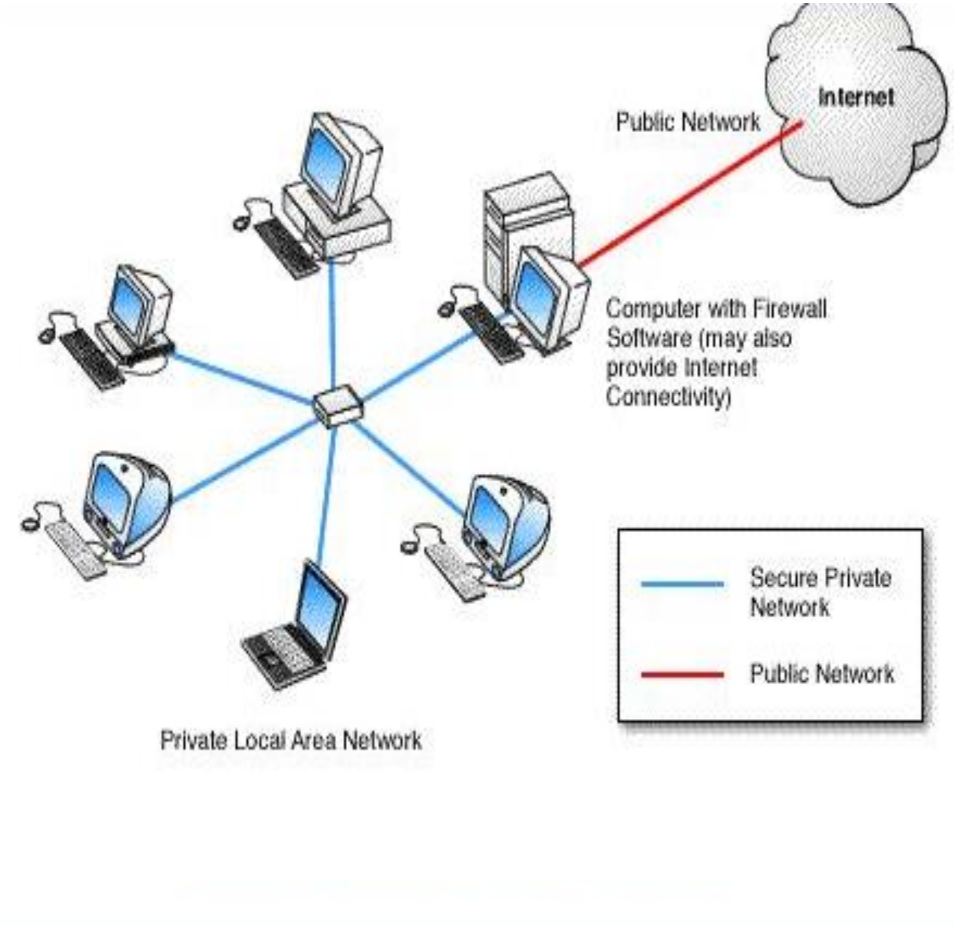
Hardware Firewalls

- 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

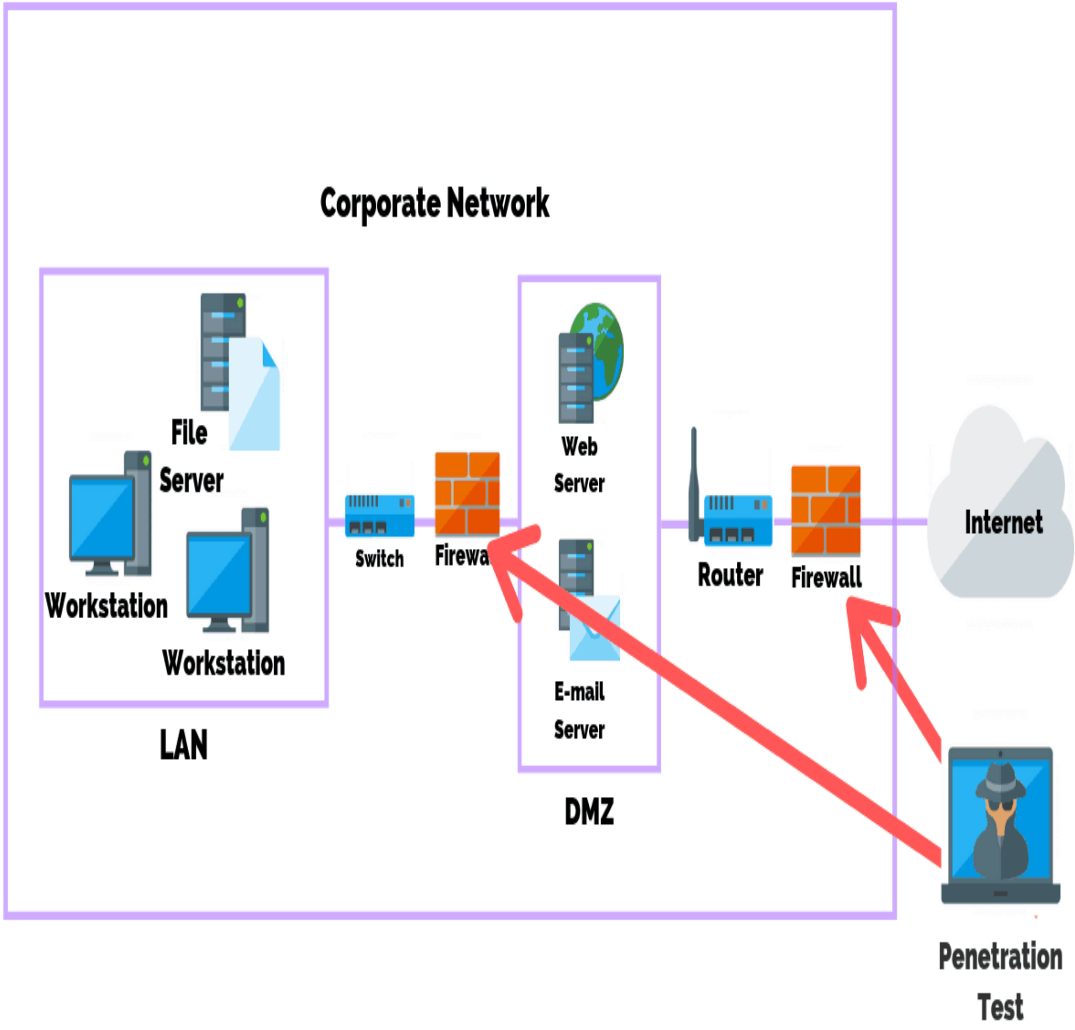

Internet
Public Network
Computer with Firewall Software (may also provide Internet Connectivity)
Secure Private Network
Public Network
Private Local Area Network

FIREWALL PENETRATION TESTING: STEPS & TOOLS

Steps To Performing A Firewall Penetration Test:

Firewall penetration testing is the process of locating, investigating and penetrating a certain firewall in order to reach the internal trusted network of a certain system.

Mostly considered to be a key part in external network penetration testing, firewall testing is one of the most important types of network tests that can be conducted as firewalls represent the first line of defense against outside intrusions.



THE STEPS USED IN FIREWALL PENETRATION TESTING ARE:

Step 1 . Locating The Firewall
Step 2 . Conducting Traceroute
Step 3 . Port Scanning
Step 4 . Banner Grabbing
Step 5 . Access Control Enumeration
Step 6 . Identifying Firewall Architecture
Step 7 . Testing The Firewall Policy
Step 8 . Firewalking
Step 9 . Port Redirection
Step10. External And Internal Testing
Step11. Test For Covert Channels
Step12. HTTP Tunneling
Step13. Identify Firewall Specific Vulnerabilities

Firewall Penetration Testing Tools

Most important tools needed for firewall penetration testing are scanners including:

- **Nmap**
- **Hping**
- **Hping2**
- **Netcat**
- **Firewalk Network Auditing tool**

These scanners allow the tester to customize packets and elicit a response from the firewall.

By interpreting the responses from the firewall, the tester can determine state of ports, services running and their version, perform banner grabbing and find vulnerabilities.

Finally, Fpipeand Datapipe tools can be used when attempting port redirection and HTTPort tool can be used when attempting HTTP tunneling.

CONCLUSION

A firewall can improve privacy by blocking access to services and the Domain Name Service in addition to lowering risks to the internal network.

A firewall can also be used to record network usage statistics and access to and from the internal network.

The most crucial element of basic security is a firewall, which requires authentication of all users and keeps track of all incoming and outgoing traffic and block the suspicious traffic based on policies and rules.

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
- https://purplesec.us/firewall-penetration-testing/

THANK YOU

PRESENTATION DESIGN

-S.HARINI
V.SRIMATHI