

## Examrace

### Discussion on Firewall in Networking Computer Science YouTube Lecture Handouts

Get unlimited access to the best preparation resource for competitive exams : [get questions, notes, tests, video lectures and more-](#) for all subjects of your exam.

Complete notes and preparation module at

[doorsteptutor.com](https://doorsteptutor.com)

Topics to Be Covered

1. Definition
2. Pictorial Representation
3. History
4. Hardware and Software Firewalls
5. Working of Firewalls
6. Rules of Firewalls
7. What can Firewalls Do?
8. What things Firewall can't do?
9. Types of Firewalls
10. Benefits of firewalls
11. Which makes firewalls fit?
12. What it protects you from?
13. MCQ

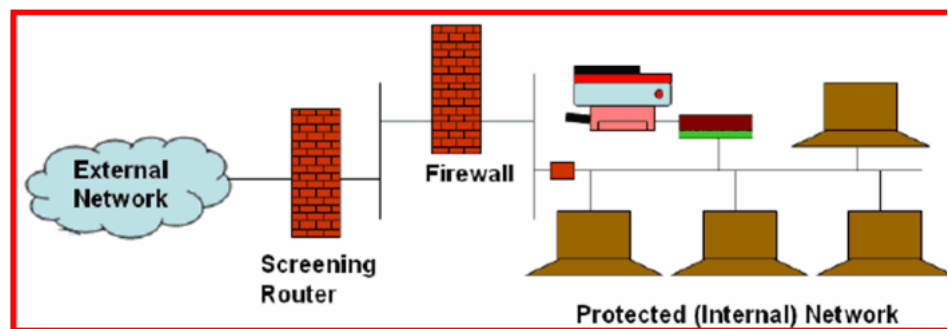
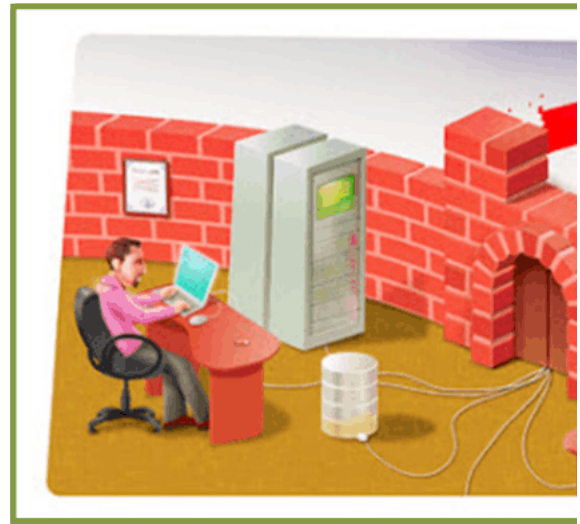
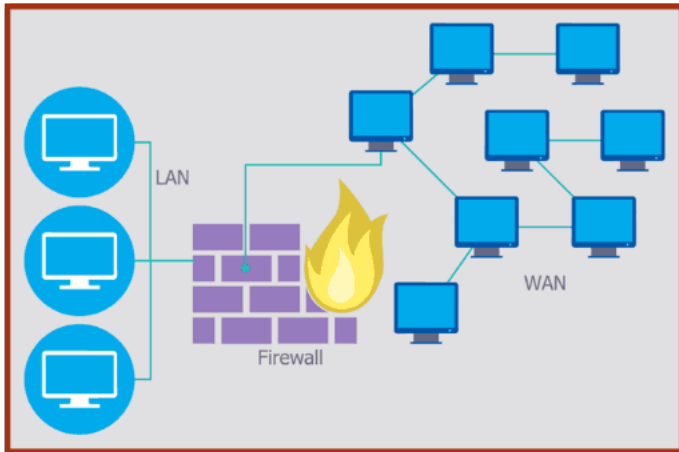
#### Definition

- **Firewall is known as that system of secure network which controls the incoming and outgoing traffic of networks, rely on predetermined security rules.**
- **It is typically helps to establish barrier between trusted and un-trusted network, i.e.. Internet.**



©Examrace.Report ©violations @<https://tips.fbi.gov/>

#### Pictorial Representation of Firewall

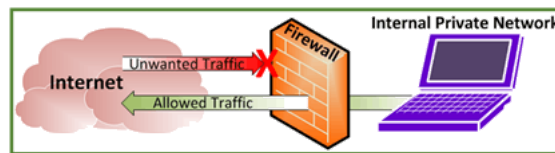
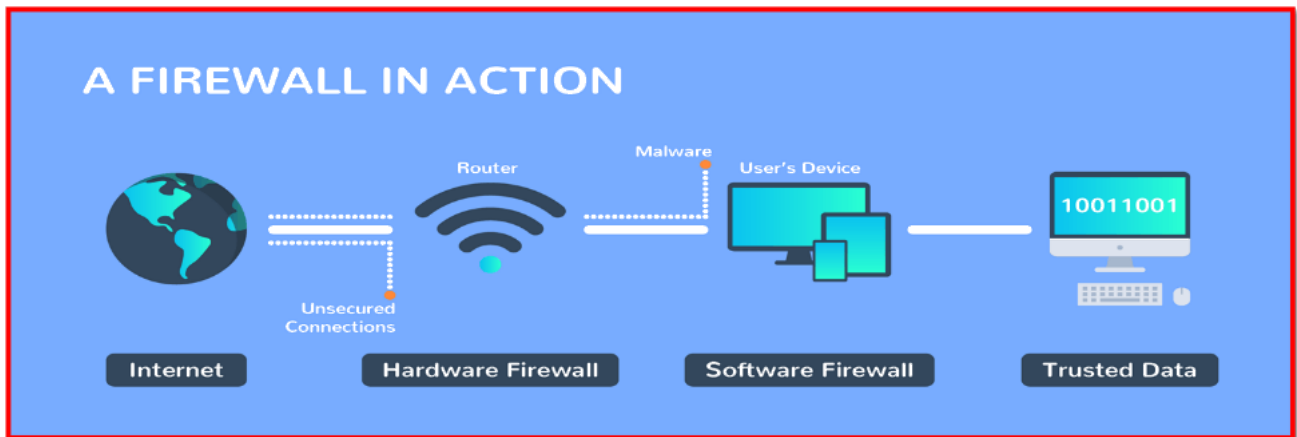


©Examrace. Report @violations @<https://tips.fbi.gov/>

### History of Firewalls

- Firewalls basically referred to a wall which intended to confine a fire within line of adjacent buildings.
- The term was applied in 1980s to technology of network which emerged when the internet was new in terms of its connectivity and global use.
- Its predecessors were routers used in late 1980s.
- Before it was used in real-life computing, it also appeared in 1983, computer hacking and war-games in movies are also inspired from its use.

Hardware and Software Firewalls Representation



### Hardware and Software Firewalls

#### Hardware Firewalls

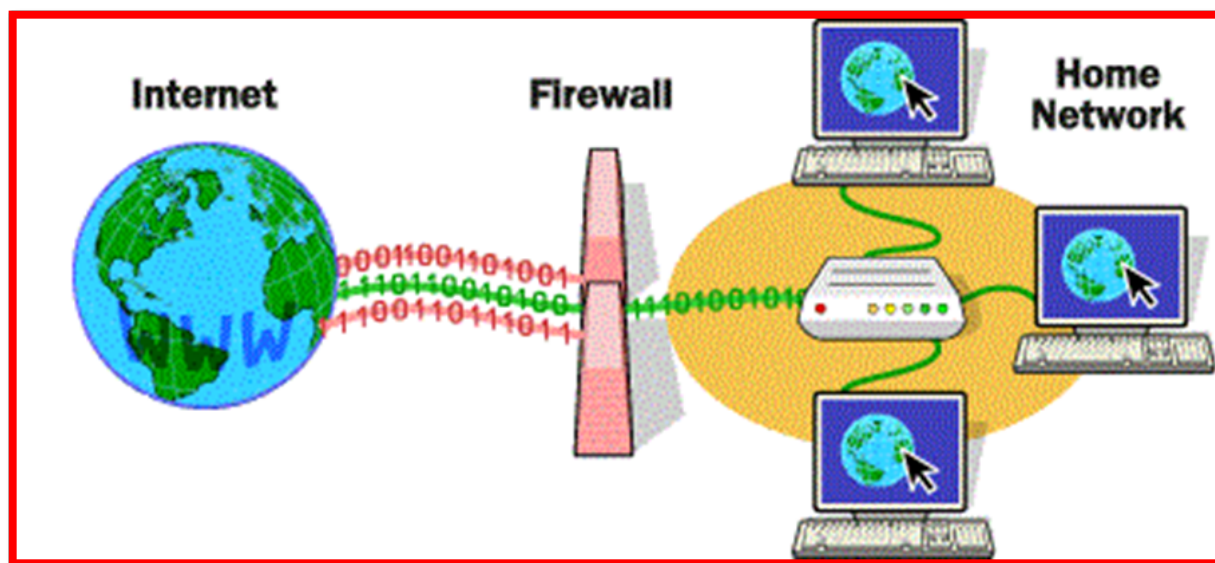
- It basically protect an entire network.
- Hardware firewalls always implemented on router level.
- It is very expensive and hard to configure.

#### Software Firewalls

- Software firewalls prefer to protect a single computer.
- It is usually less expensive and easier to configure.

### Working of Firewalls

- Inspects each individual “packet” of data as it arrives at either side of the firewall.
- Determine whether it should be allowed to pass through or if it should be blocked.



©Examrace. Report @violations @<https://tips.fbi.gov/>

### Rules of Firewalls

There are basically three rules in firewall which are given below:-

- ALLOW:- It allows the flow of traffic automatically because it has been deemed.
- BLOCK:- It blocks the traffic which has been dangerous for your computer.
- ASK:- It always ask the user throughout traffic travel whether it is allowed or not to move.

### What Can a Firewall Do?

- It always stop hackers to access computer.
- Firewalls can protect personal information.
- It is helpful to block “Pop Up” and cookies.
- It can determine which program is able to access computer.
- It blocks invalid packets.



©Examrace. Report ©violations @<https://tips.fbi.gov/>

### What a Firewalls Can't Do?

- It can't protect you against malicious insiders.
- It also cannot protect you against connection from which you cannot go through.
- Firewalls can't protect against completely new threats.
- It can't protect against viruses also.



©Examrace. Report ©violations @<https://tips.fbi.gov/>

### Types of Firewalls

There are various types of firewalls which are mentioned below:-

- Packet Filters

- Application Gateways
- State-full Inspection Firewalls
- Circuit- Level Gateways

#### Packet Filters

- It works in OSI model's network layer applies set of rules on each packet and based on results, it decides either forward or discard packet.
- Security threats to packet filters are:-
  - IP address spoofing
  - Source Routing Attacks
  - Tiny fragment attacks

#### Application Gateways

**It is basically known as Proxy Server. It works in three different steps that are given below:-**

- Step1:- User contact this gateway using protocol application, i.e.. HTTP.
- Step 2:- It asks about remote host, if user want to establish connection and also asks for username and password to access services of application gateways.
- Step 3:- After verification of user, it accesses remote host on the behalf of user for the delivery of packets.

#### Stateful Inspection Firewalls

- It is basically known as 'Dynamic Packet Filters'
- It is used to keep track of the state of active connections and uses this information to decide which packets to allow through it, i.e.. it adapts itself to current information exchange, unlike the normal packet filters/stateless packet filters, which have hardcoded routing rules.

#### Circuit-Level Gateways

- It is usually work at session layer of OSI model.
- It is advanced variation of Application Gateway.
- It works as virtual connection between remote host and internal users by creating new connection between itself and remote host.
- It changes source IP address in packet and put its own address instead of it from end users.
- IP address of internal users are hidden and secured from outside world.

#### Benefits of Firewalls

- It protects private local area network from hostile intrusion from the internet.
- It allows network administrators to offer access to specific types of internet services to selected LAN users.
- It is an essential part of any information management program and also able to access who has access to what extent.
- Privileges can be granted according to job description and need rather than on all-or-nothing basis.



©Examrace. Report @violations @<https://tips.fbi.gov/>

### Which Makes the Firewalls Fit?

- IP address
- Domain Names
- Protocols
- Ports

### What It Protects You From?

- Remote login
- SMTP session hijacking
- Operating system bugs.
- Spam
- E-mail bombs
- Source Routing

### MCQs

Q1. How many rules are comes under Firewalls?

- a) One
- b) Six
- c) Three
- d) Five.

Answer: c

Q2. Which of the following task a firewall cannot perform?

1. Stop hackers to access
2. Protect personal information.
3. Block "Pop Up" and cookies.
4. None of these.

Answer: 4

Chapters

0: 00 Firewall in Networking

0: 07 Topics to Be Covered

1: 08 Definition

2: 12 Pictorial Representation

3: 22 History of Firewalls

4: 05 Hardware and Software Firewalls Representation

4: 49 Hardware and Software Firewalls

5: 28 Working Of Firewalls

5: 49 Rules Of Firewalls

6: 36 What Can Firewalls Do?

7: 24 What Things Firewall can't Do?

8: 26 Types Of Firewalls

11: 23 Benefits Of Firewalls

12: 15 Which Makes Firewalls Fit?

12: 26 What It Protects You From?

13: 01 MCQs on Firewalls

✉ Mayank

Developed by: [Mindsprite Solutions](#)