**Module 5- Important questions**

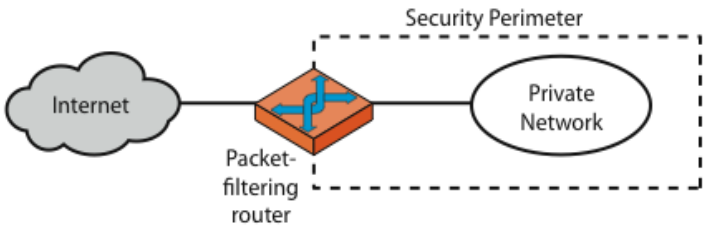
**1. What is a firewall? Explain different types of firewalls with diagram.**

A firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter, forming a single choke point where security and audit can be imposed.

Three common types of firewalls:

a. packet filters,
b. application-level gateways, &
c. Circuit-level gateways.

**a)Packet-Filtering Router**




(a) Packet-filtering router

- A packet-filtering router applies a set of rules to each incoming and outgoing IP packet to forward or discard the packet.
- Filtering rules are based on information contained in a network packet such as src & dest IP addresses, ports, transport protocol & interface. Some advantages are simplicity, transparency & speed.
- If there is no match to any rule, then one of two default policies are applied:
  - that which is not expressly permitted is prohibited (default action is discard packet), conservative policy
  - that which is not expressly prohibited is permitted (default action is forward packet), permissive policy.

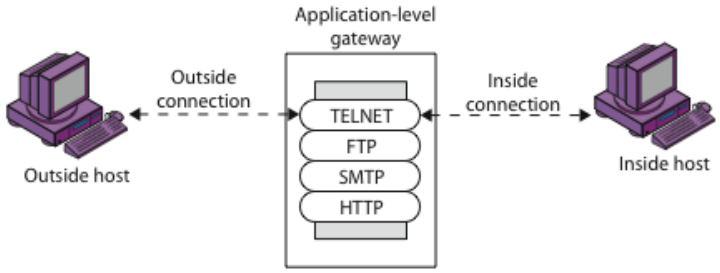
The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.

- If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard
- the packet. If there is no match to any rule, then a default action is taken.

Two default policies are possible:

- ● **Default** = *discard*: That which is not expressly permitted is prohibited.
- ● **Default** = *forward*: That which is not expressly prohibited is permitted.

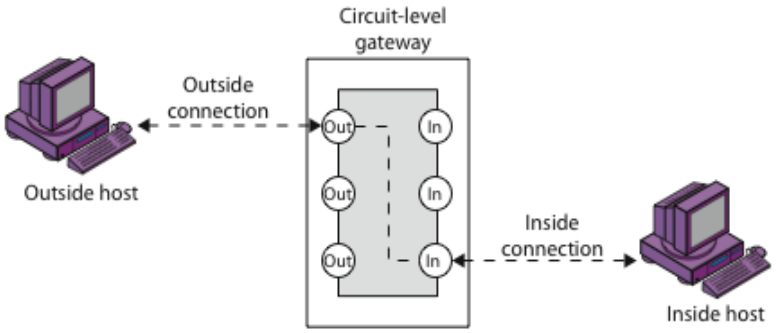
**b)Application Level Gateway (or Proxy)**




(b) Application-level gateway

- have application specific gateway / proxy
- has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
  - can log / audit traffic at application level
- need separate proxies for each service
  - some services naturally support proxying
  - others are more problematic

**c)Circuit Level Gateway**




(c) Circuit-level gateway

- relays two TCP connections
- imposes security by limiting which such connections are allowed
- once created usually relays traffic without examining contents
- typically used when trust internal users by allowing general outbound connections
- One of the most common circuit-level gateways is SOCKS.

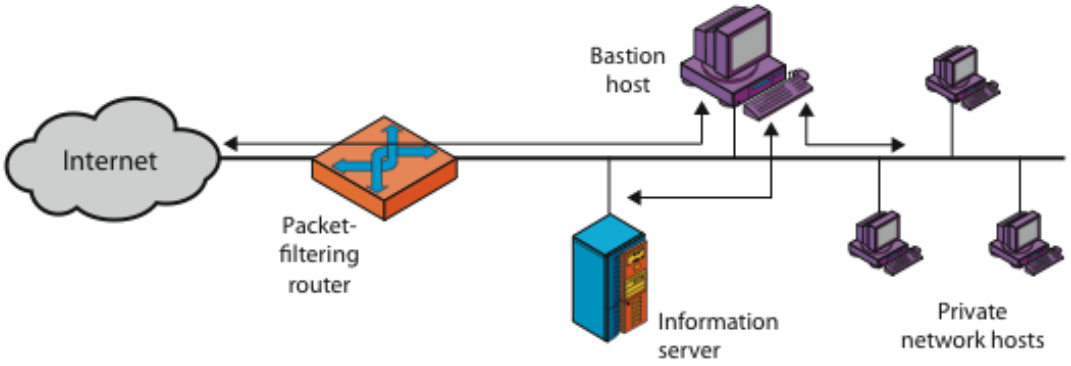
SOCKS consists of the following components:
● The SOCKS server, which runs on a UNIX-based firewall.
● The SOCKS client library, which runs on internal hosts protected by the firewall.
● SOCKS-ified versions of several standard client programs such as FTP and TELNET.

**2.Describe the different Firewall Configurations with diagrams.**

**Three common firewall configurations:**

1.screened host firewall, single-homed bastion configuration
2. Screened host firewall, dual-homed bastion configuration
3. Screened subnet firewall configuration

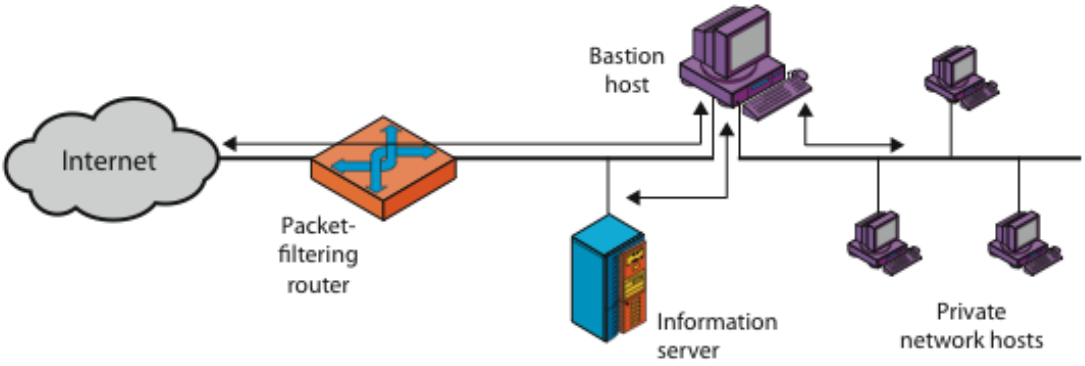
**1. Screened host firewall, single-homed bastion configuration:**




(a) Screened host firewall system (single-homed bastion host)

- Consists of two systems:
  - a **packet-filtering router** - allows Internet packets to/from bastion only
  - a **bastion host** - performs authentication and proxy functions
- This configuration has greater security, as it implements both packet-level & application-level filtering, forces an intruder to generally penetrate two separate systems to compromise internal security.
- Also affords flexibility in providing direct Internet access to specific internal servers (e.g. web) if desired.

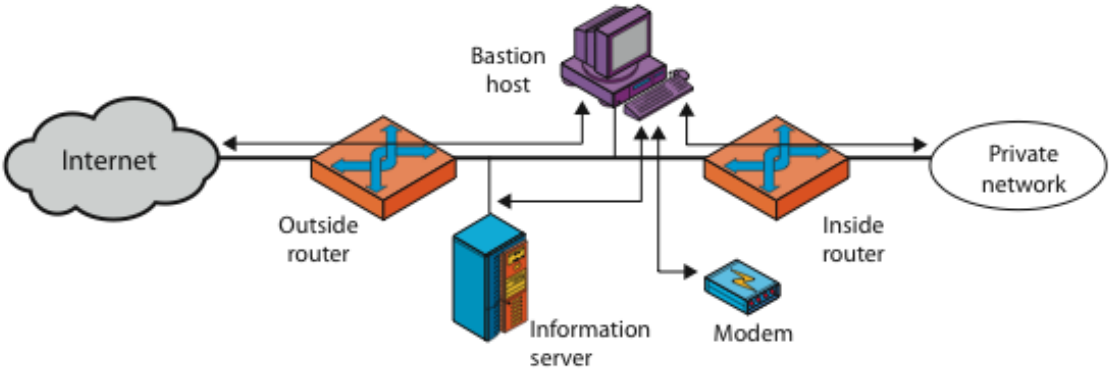
**2. Screened host firewall, dual-homed bastion configuration:**




(b) Screened host firewall system (dual-homed bastion host)

- Physically separates the external and internal networks, ensuring two systems must be compromised to breach security.
- The advantages of dual layers of security are also present here.
- Again, an information server or other hosts can be allowed direct communication with the router if this is in accord with the security policy, but are now separated from the internal network.

**3. Screened subnet firewall configuration**




(c) Screened-subnet firewall system

- It has two packet-filtering routers, one between the bastion host and the Internet and the other between the bastion host and the internal network, creating an isolated sub network.
- This may consist of simply the bastion host but may also include one or more information servers and modems for dial-in capability.
- Typically, both the Internet and the internal network have access to hosts on the screened subnet, but traffic across the screened subnet is blocked.

**3. Explain four phases of handshake protocol with diagram.**

- The most complex part of SSL is the Handshake Protocol.