Firewalls

Why do we need Firewalls?

Internet connectivity is a must for most people and organizations

- especially for me

But a convenient Internet connectivity is an invitation for intruders and hackers

- yet another example of tradeoff between convenience and security

Firewall basically provides us an option to play within the spectrum of this tradeoff

What is a Firewall?

Effective means of protecting local network of systems from network-based security threats from outer world

- while providing (limited) access to the outside world (the Internet)

Firewall Basics

The firewall is inserted between the internal network and the Internet (a choke point)

- Establish a controlled link and protect the network from Internet-based attacks
  - keeps unauthorized users away,
  - imposes restrictions on network services; only authorized traffic is allowed
- Location for monitoring security-related events
  - auditing, alarms can be implemented
- some firewalls supports IPSec, so VPNs can be implemented firewall-to-firewall
- some firewalls support NAT

Open discussion: can’t we put one firewall for each station within the local network? What are pros and cons?

Firewall Characteristics - 1

Design goals:

- All traffic to/from inside from/to outside must pass through the firewall
- Only authorized traffic (defined by the local security policy) will be allowed to pass
- The firewall itself should be immune to penetration (use of trusted system with a secure operating system)

Firewall Characteristics - 2

General techniques for access control

- Service control
  - Determines the types of Internet services that can be accessed
    - Mostly using TCP/UDP port numbers
  - Direction of traffic is important for the decision
    - Some services are open for outbound, but not inbound (or vice versa)
- User control
  - Controls access to a service according to which user is attempting to access it
  - need to authenticate users. This is easy for internal users, but what can be done for external ones?
- Behavior control
  - Controls how particular services are used (e.g. filter e-mail for spam control)
  - More advanced: Deep Packet Inspection (DPI)
    - Port 80 (HTTP) is used for multiple services: web mail, social media, etc.
    - DPI is to effectively and efficiently check the content of the packet to see what type of application it contains

Types of Firewalls

Packet-filtering firewall

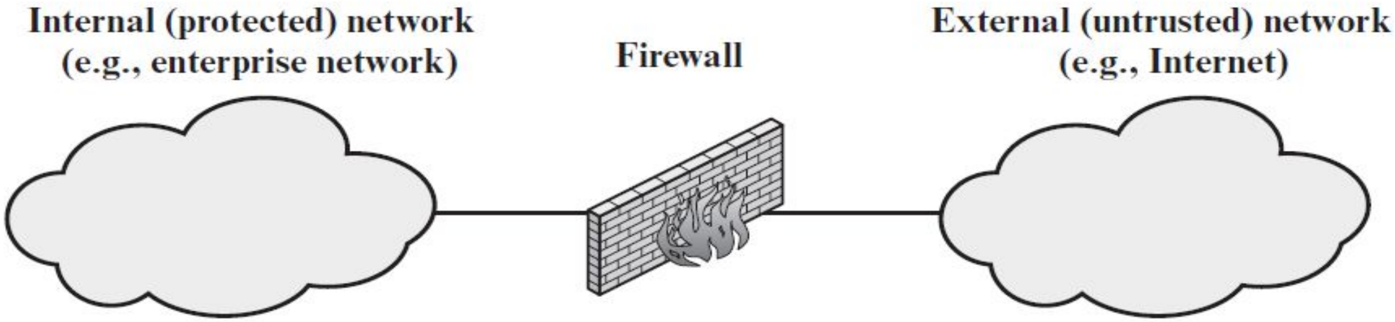
Stateful Inspection Firewall

Proxy Firewalls

- Application-level gateways
- Circuit-level gateways

Packet-filtering Firewall

- Foundation of any firewall system
- Applies a set of rules to each incoming/outgoing IP packet and then forwards (permits) or discards (denies) the packet (in both directions)
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- context is not checked
- Two default policies (permit or deny)



Internal (protected) network
(e.g., enterprise network)

Firewall

External (untrusted) network
(e.g., Internet)

Packet-filtering Firewall

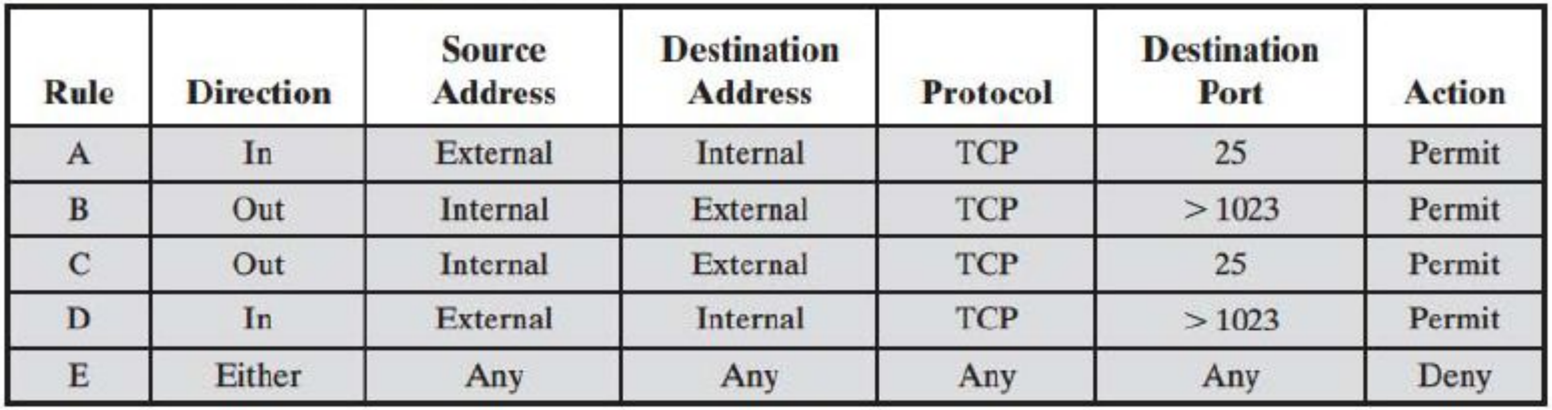
Filtering rules are based on

- Source and Destination IP addresses
- Source and Destination ports (services) and transport protocols (TCP or UDP)

Rules are listed and a match is tried to be found starting with the first rule

- Action is either permit or deny
- Generally first matching rule is applied
- If no match, then default policy is used
  - Default is either deny or permit

Packet Filtering Examples - 1



Rule	Direction	Source Address	Destination Address	Protocol	Destination Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	> 1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	> 1023	Permit
E	Either	Any	Any	Any	Any	Deny

A: incoming SMTP traffic allowed from particular "External" IP addresses to particular "Internal" IP addresses

- B: aimed to allow the response packets (problematic)

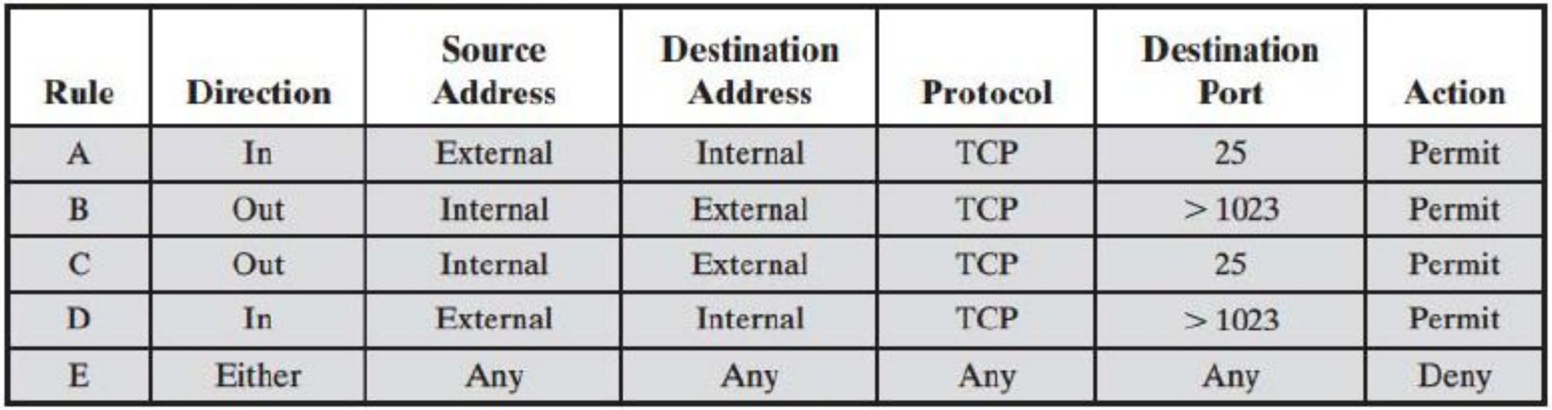
C: Outgoing SMTP traffic allowed from particular "Internal" IP addresses to particular "External" IP addresses

- D: aimed to allow the response packets (problematic)

E: Default rule: deny (discard) the rest

- Of course in a normal firewall there must be other "permit" rules for proper operation of other services

Packet Filtering Examples - 2



Rule	Direction	Source Address	Destination Address	Protocol	Destination Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	> 1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	> 1023	Permit
E	Either	Any	Any	Any	Any	Deny

Rules B and D are problematic

Rule D allows not only incoming SMTP responses, but any packet with destination port >1023

- Malicious services use >1023 destination ports

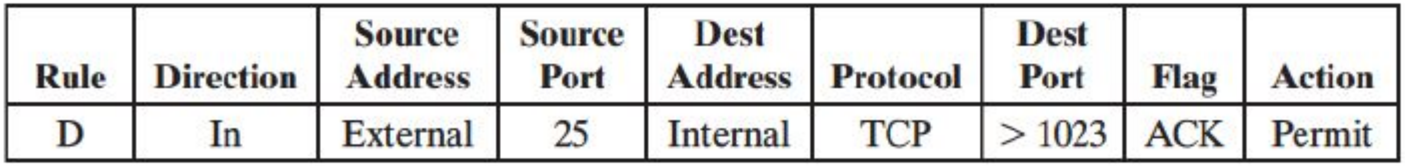
Solution: add source port to the rule set in order to set the application for response packets

- For Rules B and D, source port is 25; for Rules A and C source port is >1023

Packet Filtering Examples - 3

Rule D is still problematic after adding source port value

- The malicious traffic may mimic source port 25 and uses >1023 destination port
- To resolve this issue we have to make sure that responses to SMTP requests is the ones to our requests; not a new traffic
  - Adding "TCP flag" field to the rule set helps
  - If ack flag is set, it is ack to our packet



Rule	Direction	Source Address	Source Port	Dest Address	Protocol	Dest Port	Flag	Action
D	In	External	25	Internal	TCP	> 1023	ACK	Permit

Another helper is stateful inspection (next slide)

Weakness

Do not examine **upper layer data**

Cannot **prevent attacks** that employ **application-specific vulnerabilities or functions**

Because of **limited information** available to the firewall, the **logging functionality** present in packet filtering firewalls is limited.

Most **packet filter firewall do not support advanced user authentication schemes**

Packet filter firewalls are generally **vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack**

Due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations

Attacks made in packet filtering firewalls

IP address spoofing

Source routing attacks

Tiny fragments attacks

Stateful Inspection

Example D shows that

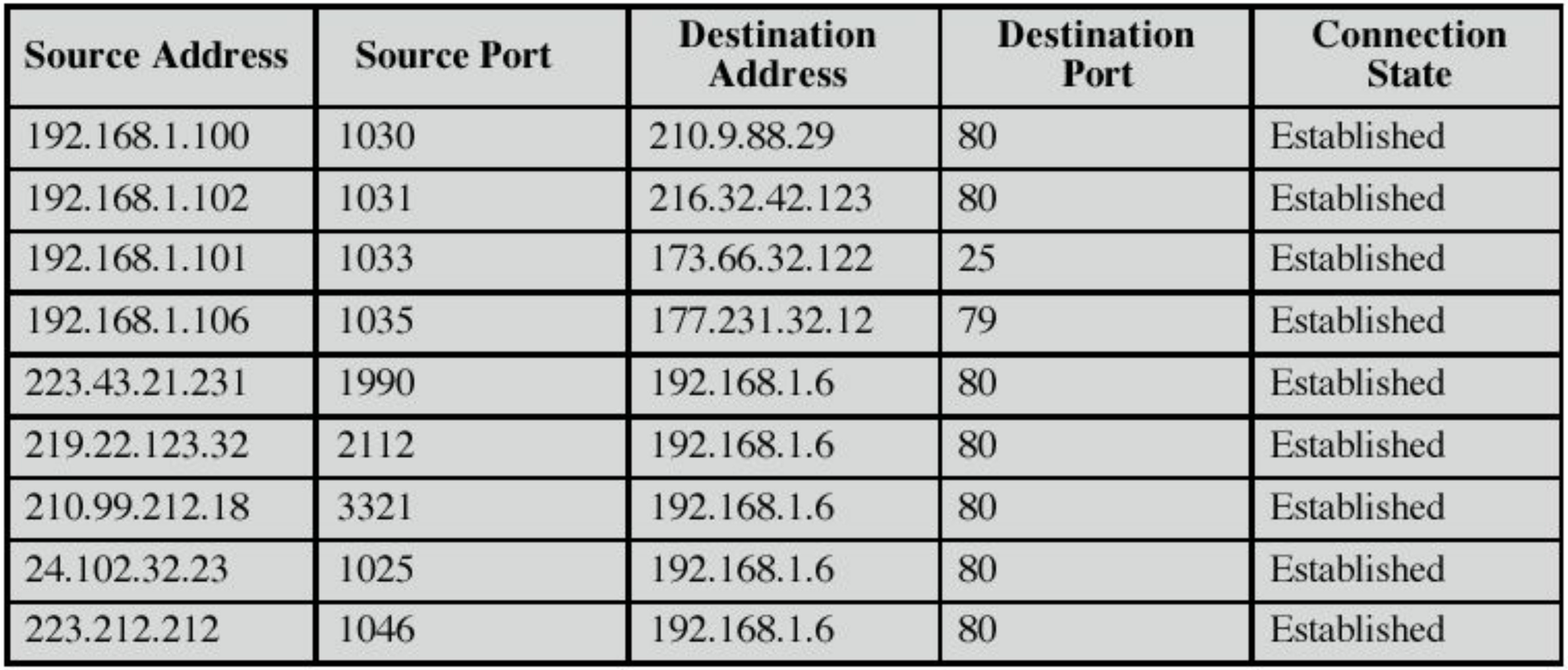
>1024 ports need to be opened

- not only due to SMTP, all services have such a structure
  - <1024 ports are for servers, a client using a service should use a local port number between 1024 and 16383

So the firewall should keep track of the currently opened >1024 ports

A *stateful inspection firewall* keeps track of outbound TCP connections with local port numbers in a table and allow inbound traffic for >1024 ports if there is an entry in that table (see next slide for an example table)

Stateful Inspection



Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.212.212	1046	192.168.1.6	80	Established

Proxy Firewall

- A proxy, in general, acts on behalf of its client.
- Proxy as an application process sits between a client and a server process.
- To The client, the proxy appears to be the server, and to the application server, the proxy appears to be a client.
  - Application Level Proxy Firewall
  - Circuit Level proxy Firewall

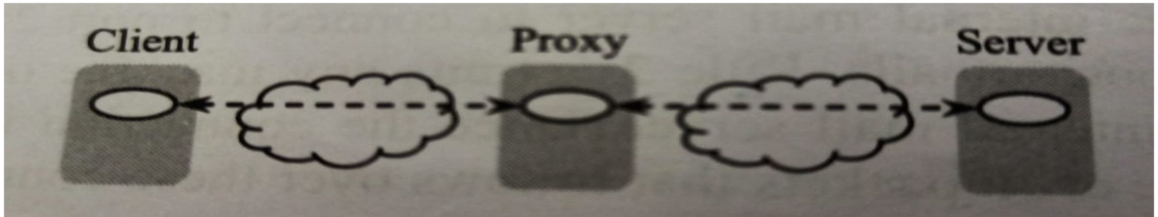


Figure 22.5 Proxy.

- ❑Application Level proxy protects security interest by scrutinizing application layer data that is exchanges between the client and server.
- ❑The circuit level proxy firewall, on the other end operates at access level.
  - ❑ It authenticates the client
  - ❑ Check authorization of the client

Application-Level Gateway

- ❑ Called a proxy server
- ❑ Acts as a relay of application-level traffic
- ❑ User contacts the gateway using a TCP/IP application, such as Telnet or FTP
- ❑ Gateway asks the user for the name of the remote host to be accessed
- ❑ More secure than packet filtering firewall

Application-level Gateway

Application-level Gateway (proxy server)

- Acts as a relay of application-level traffic

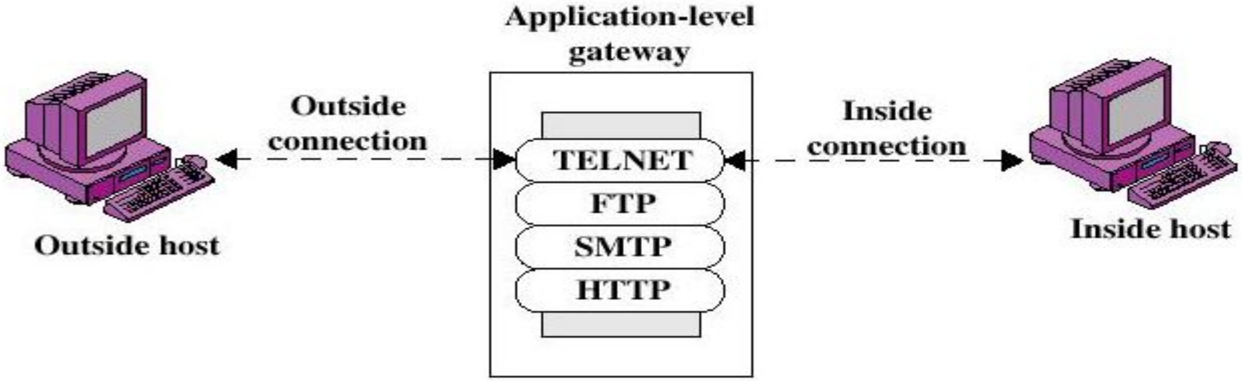
Proxy obtains application specific information from the user and relays to the server

- Optionally authenticates the users

Only allowable applications can pass through

- Feature-based processing is possible

Additional processing overhead on each connection

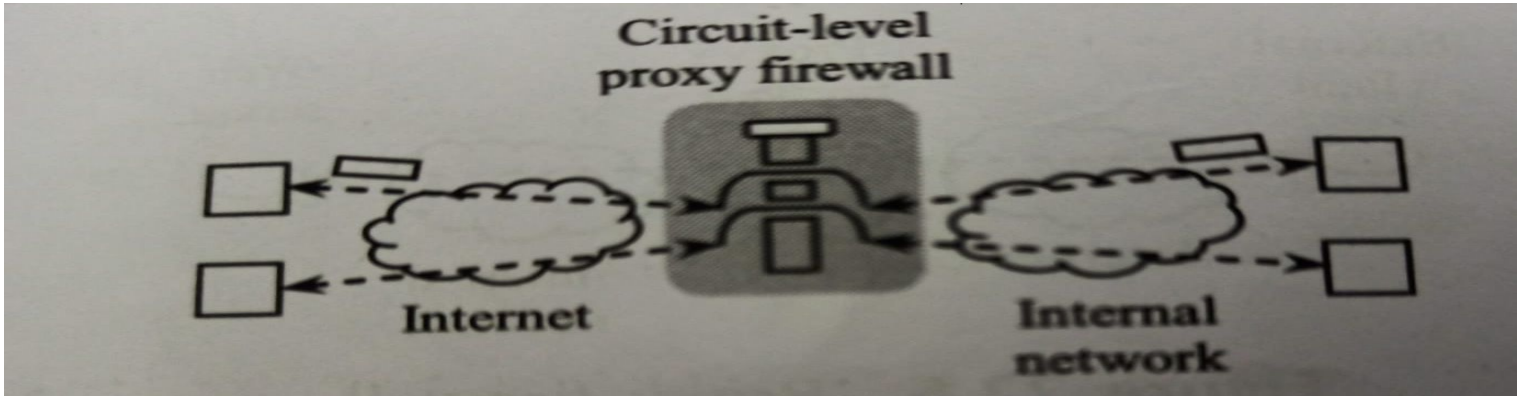


Disadvantage

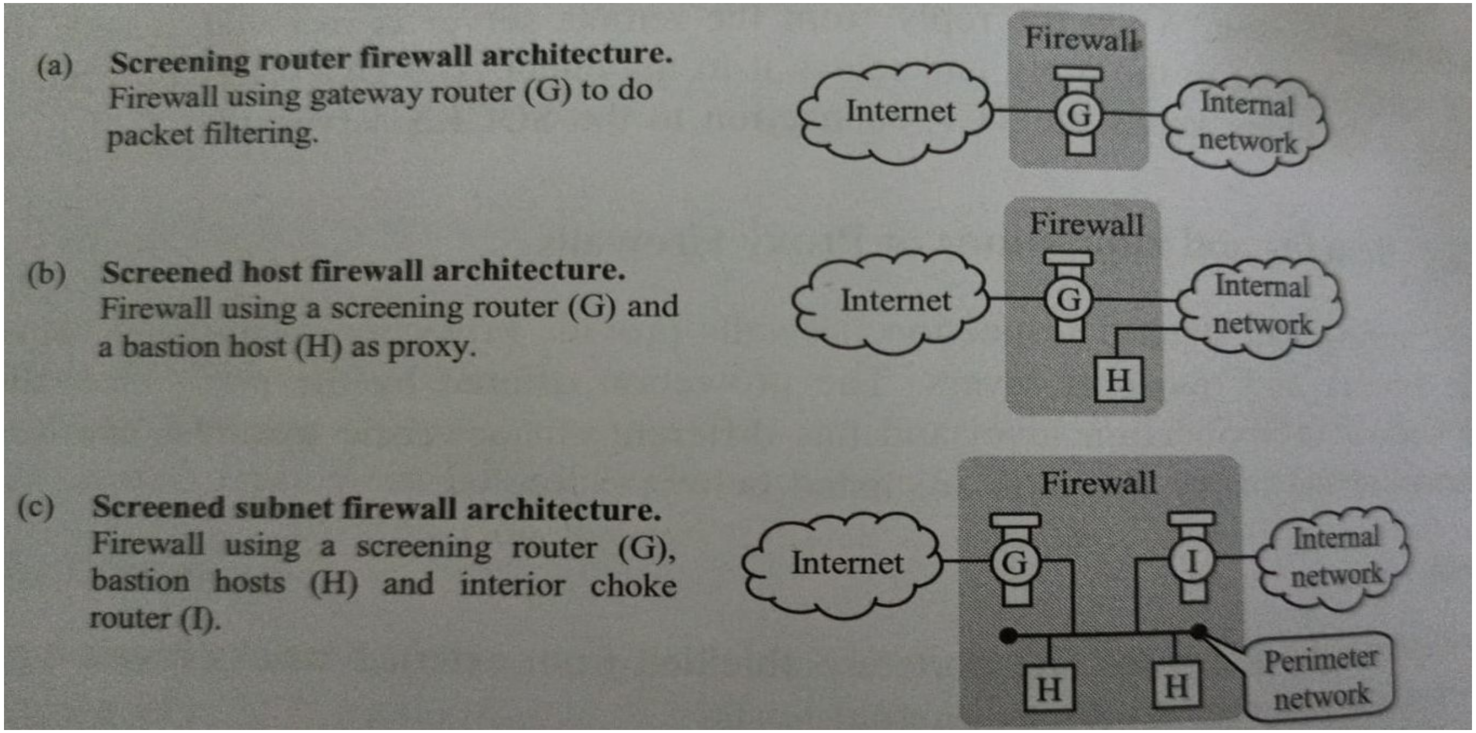
- Additional overhead

Circuit-Level Proxy Firewall

- It Authenticates the client and provides access, and further relays the message between them.
- It carries out relaying function by building association between the external and internal connections



Firewall Architecture



(a) **Screening router firewall architecture.** Firewall using gateway router (G) to do packet filtering.

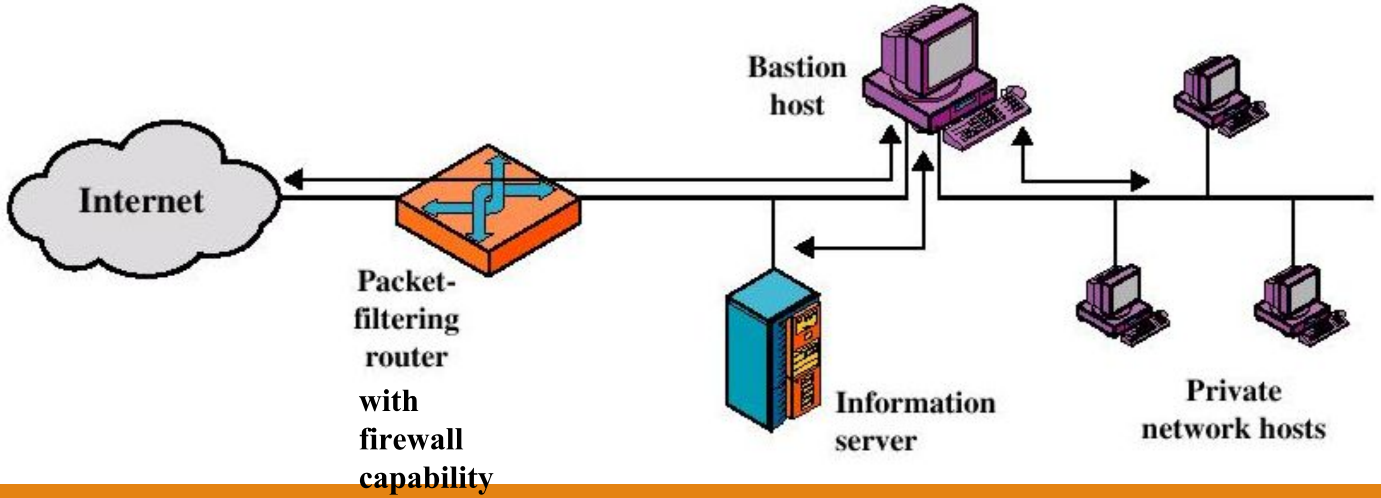
(b) **Screened host firewall architecture.** Firewall using a screening router (G) and a bastion host (H) as proxy.

(c) **Screened subnet firewall architecture.** Firewall using a screening router (G), bastion hosts (H) and interior choke router (I).

Screened host firewall system (dual-homed bastion host)

Only packets from and to the bastion host are allowed to pass through the router

The bastion host performs authentication and proxy functions



Dual-homed Bastion Host

Good security because of two reasons:

- This configuration implements both packet-level and application-level filtering
- An intruder must generally penetrate two separate systems in order to get to the internal network

This configuration also has flexibility in providing direct Internet access to a public information server, e.g. Web server

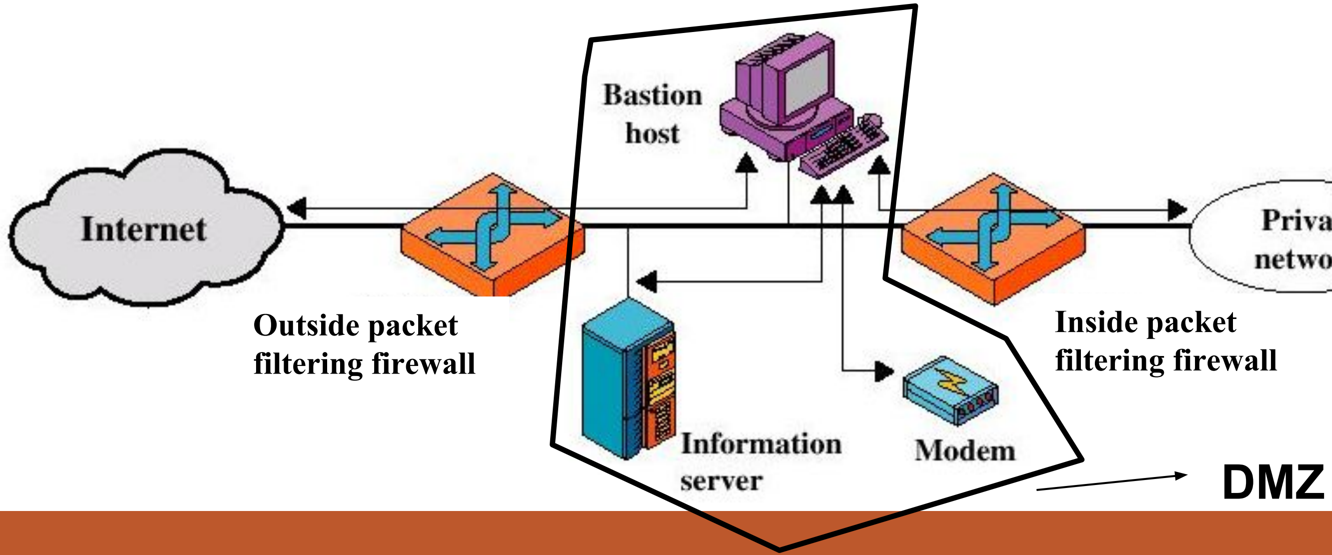
- by configuring the packet filtering router

Screened-subnet Firewall System

creates an isolated sub-network between firewalls

- Internet and private network have access to this subnet
- Traffic across the subnet is blocked
- This subnet is the DMZ (demilitarized zone)

Internal network is invisible to the Internet


Bastion host
Internet
Private network
Outside packet filtering firewall
Inside packet filtering firewall
Information server
Modem
DMZ