# Information Systems Security

Dr. Ayman Abdel-Hamid

College of Computing and Information Technology

Arab Academy for Science & Technology and
Maritime Transport

## Chapter 20

## Firewalls

# Outline

- Firewalls
  - Types
  - Configurations
  - Access control
  - Trusted systems

# Introduction

- seen evolution of information systems
- now everyone wants to be on the Internet
- and to interconnect networks
- has persistent security concerns
  - can’t easily secure every system in org.
- need "harm minimization"
- a **Firewall** usually part of this

# What is a Firewall?

- a **choke point** of control and monitoring
- interconnects networks with differing trust
- imposes restrictions on network services
  - only authorized traffic is allowed
- auditing and controlling access
  - can implement alarms for abnormal behavior
- is itself immune to penetration
- provides **perimeter defence**

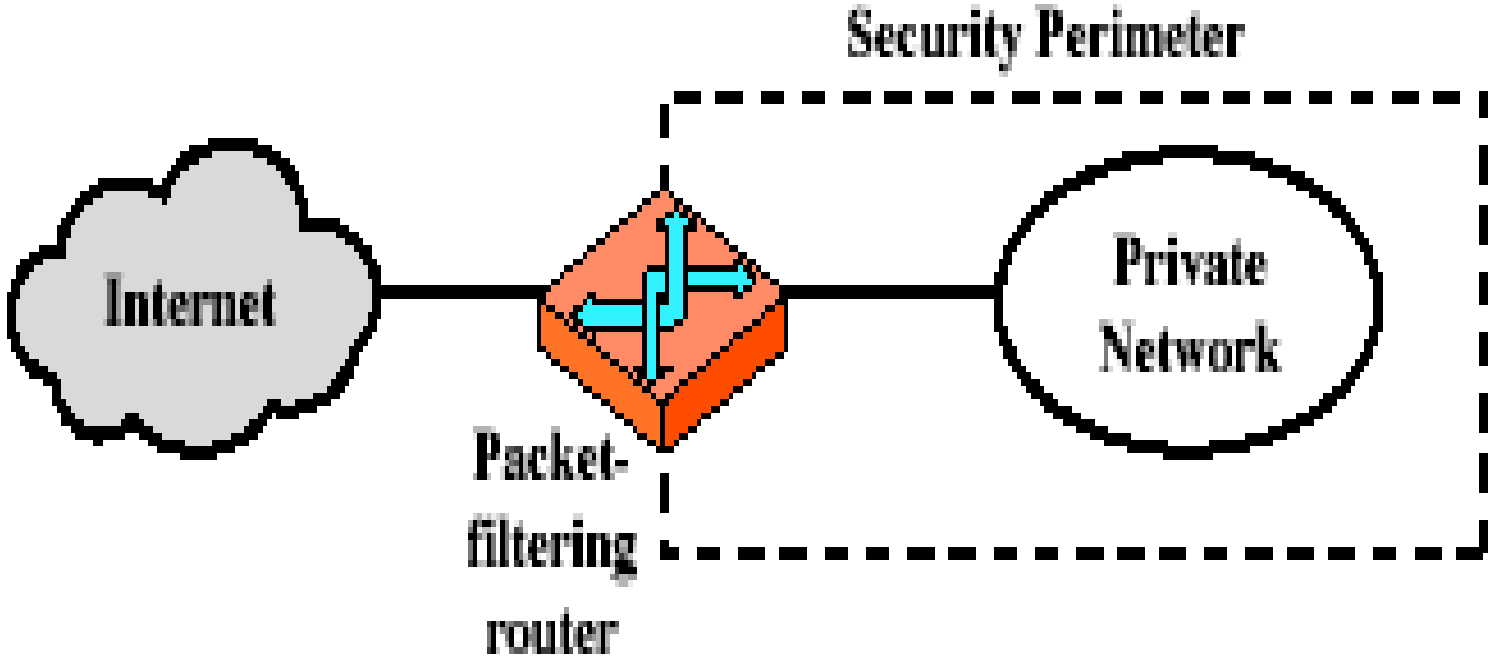
# Firewall Techniques for Access Control

- Service Control
  - Types of internet services accessed inbound or outbound
- Direction Control
  - Direction in which particular service requests may be initiated and allowed to flow through the firewall
- User Control
  - Controls access to service according to which user is attempting to access it
- Behaviour Control
  - How particular services are used

# Firewall Limitations

- cannot protect from attacks bypassing it
  - e.g. utility modems, trusted organisations, trusted services (eg SSL/SSH)
- cannot protect against internal threats
  - e.g. disgruntled employee
- cannot protect against transfer of all virus infected programs or files
  - because of huge range of O/S & file types

# Firewalls – Packet Filters




(a) Packet-filtering router

# Firewalls – Packet Filters

- foundation of any firewall system
- examine each IP packet in both directions (no context) and permit or deny according to rules
  - Source IP address
  - Destination IP address
  - Source and destination ports
  - IP protocol field
  - Interface
- If no rule match → possible default policies
  - that not expressly permitted is prohibited
  - that not expressly prohibited is permitted

# Firewalls – Packet Filters

**Table 20.1 Packet-Filtering Examples**

**A**

| action | ourhost | port | theirhost | port | comment |
|---|---|---|---|---|---|
| block | * | * | SPIGOT | * | we don't trust these people |
| allow | OUR-GW | 25 | * | * | connection to our SMTP port |

**B**

| action | ourhost | port | theirhost | port | comment |
|---|---|---|---|---|---|
| block | * | * | * | * | default |

**C**

| action | ourhost | port | theirhost | port | comment |
|---|---|---|---|---|---|
| allow | * | * | * | 25 | connection to their SMTP port |

**D**

| action | src | port | dest | port | flags | comment |
|---|---|---|---|---|---|---|
| allow | {our hosts} | * | * | 25 | | our packets to their SMTP port |
| allow | * | 25 | * | * | ACK | their replies |

**E**

| action | src | port | dest | port | flags | comment |
|---|---|---|---|---|---|---|
| allow | {our hosts} | * | * | * | | our outgoing calls |
| allow | * | * | * | * | ACK | replies to our calls |
| allow | * | * | * | >1024 | | traffic to nonservers |

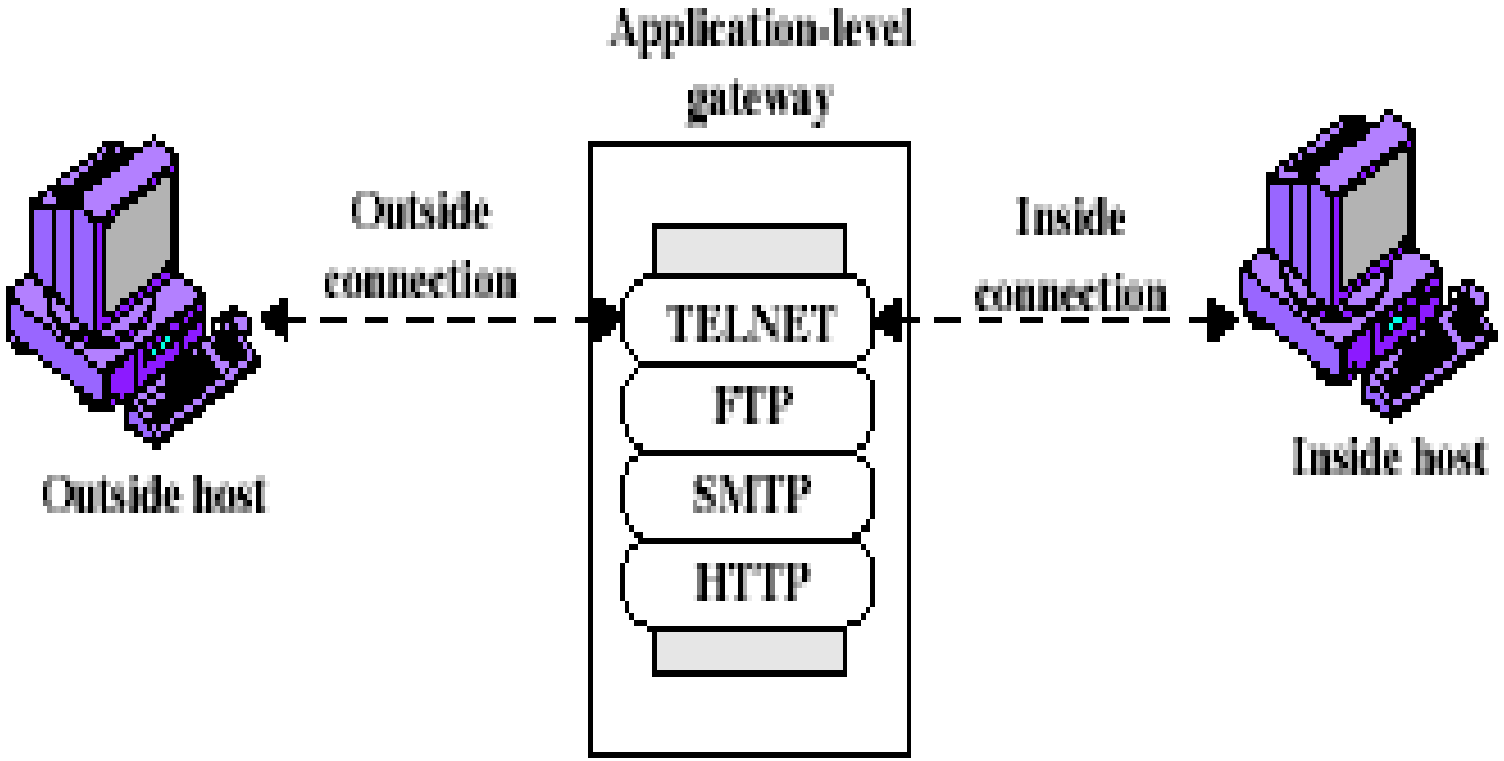
# Attacks on Packet Filter Firewalls

- IP address spoofing
  - fake source address to be trusted (address of internal host)
  - *add filters on router to block (discard packet with an inside source address if packet arrives on external interface)*
- source routing attacks
  - attacker sets a route other than default
  - *block source routed packets*
- tiny fragment attacks
  - split header info over several tiny packets (force TCP header information into a separate packet fragment)
  - *either discard or reassemble before check*

# Firewalls – Stateful Packet Filters

- Traditional packet filter does not take into consideration higher layer context
- examine each IP packet in context
  - keeps tracks of client-server sessions
  - checks each packet validly belongs to one
- better able to detect bogus packets out of context

# Firewalls - Application Level Gateway (or Proxy)

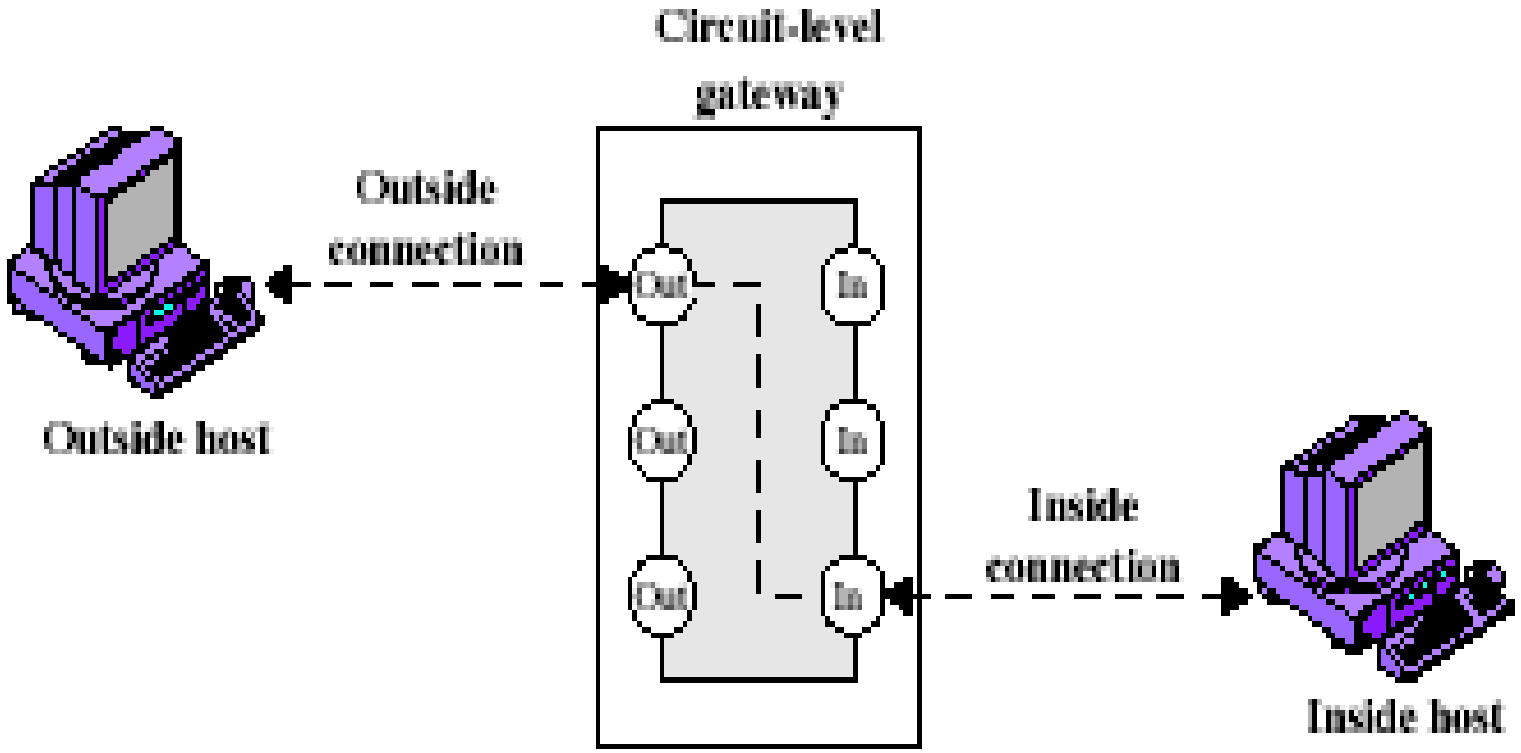



(b) Application-level gateway

# Firewalls - Application Level Gateway (or Proxy)

- use an *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
- need separate proxies for each service
  - some services naturally support proxying
  - others are more problematic
  - custom services generally not supported

# Firewalls - Circuit Level Gateway




(c) Circuit-level gateway

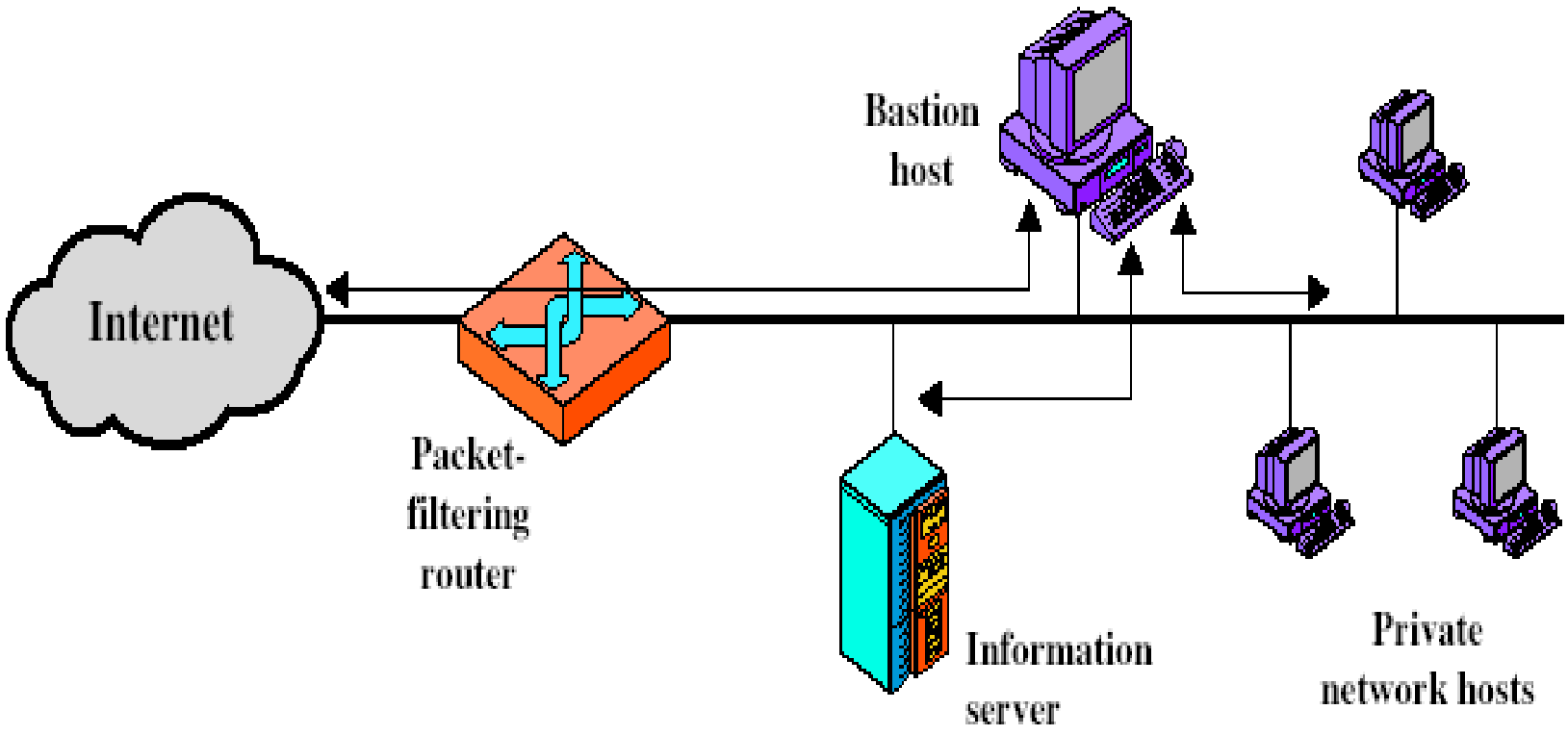
# Firewalls - Circuit Level Gateway

- 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

# Bastion Host

- highly secure host system
- potentially exposed to "hostile" elements
- hence is secured to withstand this
- may support 2 or more Net. connections
- may be trusted to enforce trusted separation between network connections
- runs circuit / application level gateways
- or provides externally accessible services

# Firewall Configurations

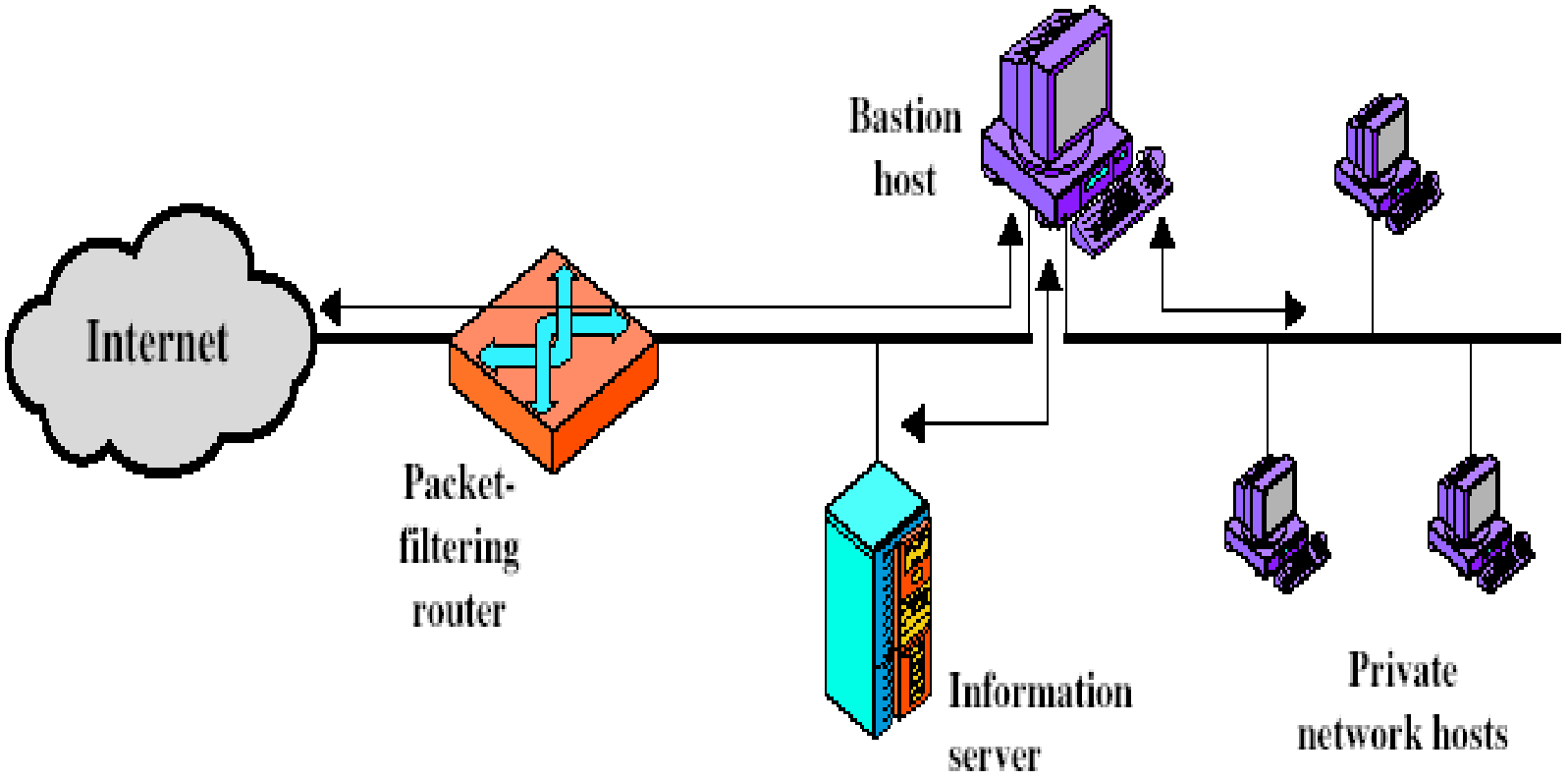



(a) Screened host firewall system (single-homed bastion host)

# Screened Host Firewall, Single-homed Bastion

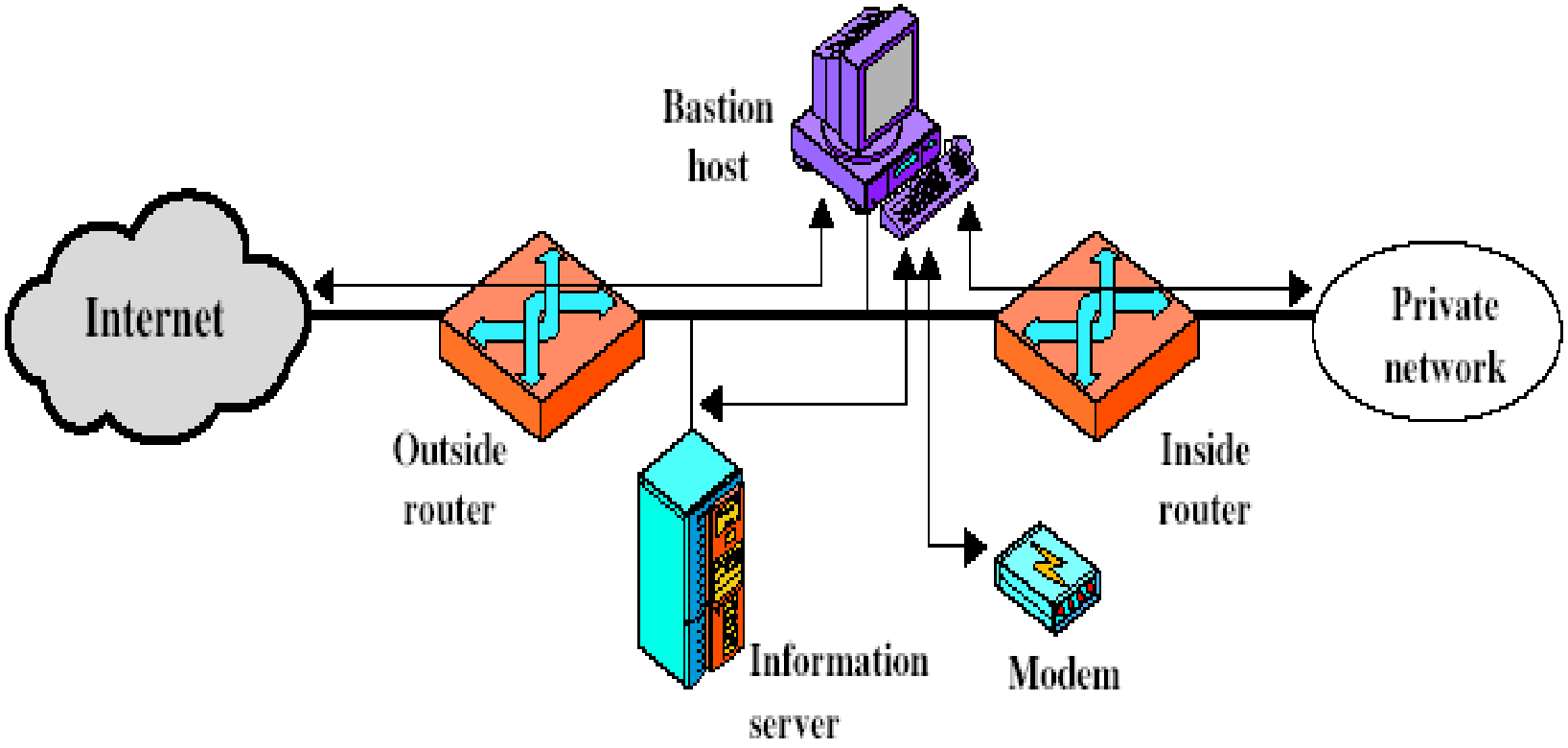
- *For traffic from the Internet*, only IP packets destined for the bastion host are allowed in
- *For traffic from internal network*, only IP packets from bastion host are allowed out
- Bastion host performs authentication and proxy functions
- Provides flexibility in allowing direct internet access (for a web server for example)
- Problem: if packet-filtering router compromised, traffic could flow directly through router

# Firewall Configurations




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

# Firewall Configurations




(c) Screened-subnet firewall system

# Screened-subnet firewall system

- 3 levels of defence
- Outside router advertises only existence of screened subnet to the Internet (Internal network invisible)
- Inside router advertises existence of screened subnet to the internal network