# Cryptography

MCA SEMESTER-IV

Paper Code: MCACS4T15

## Unit : 4 - System Security

## Intrusion Prevention Systems

**Ms. Sushmita Chakraborty**
**Assistant Professor**
**Dept. of MCA, Patna Women's College**
**Emai-id:** sush123.chakraborty@gmail.com

- Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity.
- Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

# Classifications

**Intrusion prevention systems can be classified into four different types:**

- Network-based intrusion prevention system (NIPS): monitors the entire network for suspicious traffic by analyzing protocol activity.
- Wireless intrusion prevention systems (WIPS): monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.
- Network behavior analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations.
- Host-based intrusion prevention system (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

## Detection methods

The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based, and stateful protocol analysis.

## Signature-Based Detection:

This method of detection utilizes signatures, which are attack patterns that are preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic for matches to these signatures. Once a match is found the intrusion prevention system takes the appropriate action. Signatures can be exploit-based or vulnerability-based. Exploit-based signatures analyze patterns appearing in exploits being protected against, while vulnerability-based signatures analyze vulnerabilities in a program, its execution, and conditions needed to exploit said vulnerability.

## Statistical anomaly-based detection:

This method of detection baselines performance of average network traffic conditions. After a baseline is created, the system intermittently samples network traffic, using statistical analysis to compare the sample to the set baseline. If the activity is outside the baseline parameters, the intrusion prevention system takes the appropriate action.

## Stateful Protocol Analysis Detection:

This method identifies deviations of protocol states by comparing observed events with "predetermined profiles of generally accepted definitions of benign activity."

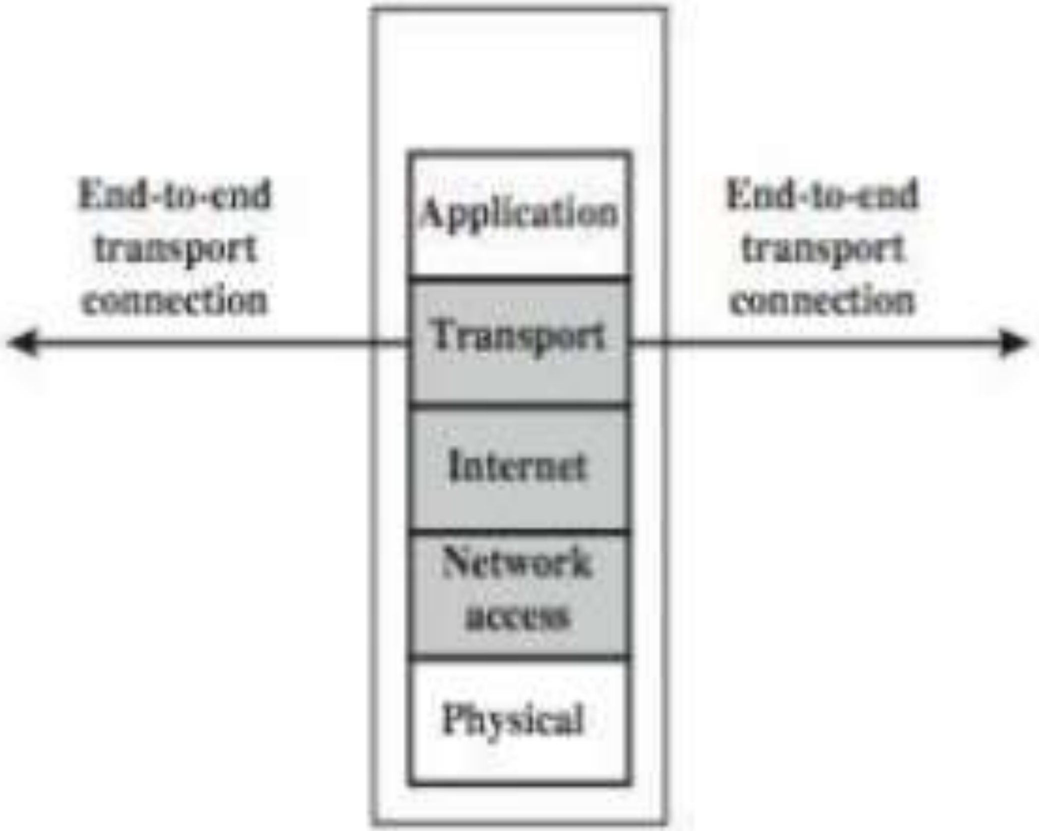
# Introduction and Overview

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

**There are several types of firewall techniques:**

- Packet filter:
- Application gateway:
- Circuit-level gateway:
- Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

# Packet Filtering Firewall


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection

# Packet Filtering Firewall

- A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet al address
- nd then forwards or discards and the packet,
- Filtering rules are based on informing contained in a network packet.
  - ✓ Source IP address
  - ✓ Destination IP address
  - ✓ Source and destination transport level address
  - ✓ IP protocol field
  - ✓ Interface

# Packet Filtering Firewall

- Two default policies are there to take default action to determine whether to forward or discard the packet.

  **Default= discard**

  **Default = forward**

- Some possible attacks on firewall:

✓ IP address spooling

✓ Source routing attacks

✓ Tiny fragment attacks

# Packet Filtering Firewall

- **Advantages:**

✓ Cost

✓ Low resource usage

✓ Best suited for smaller network

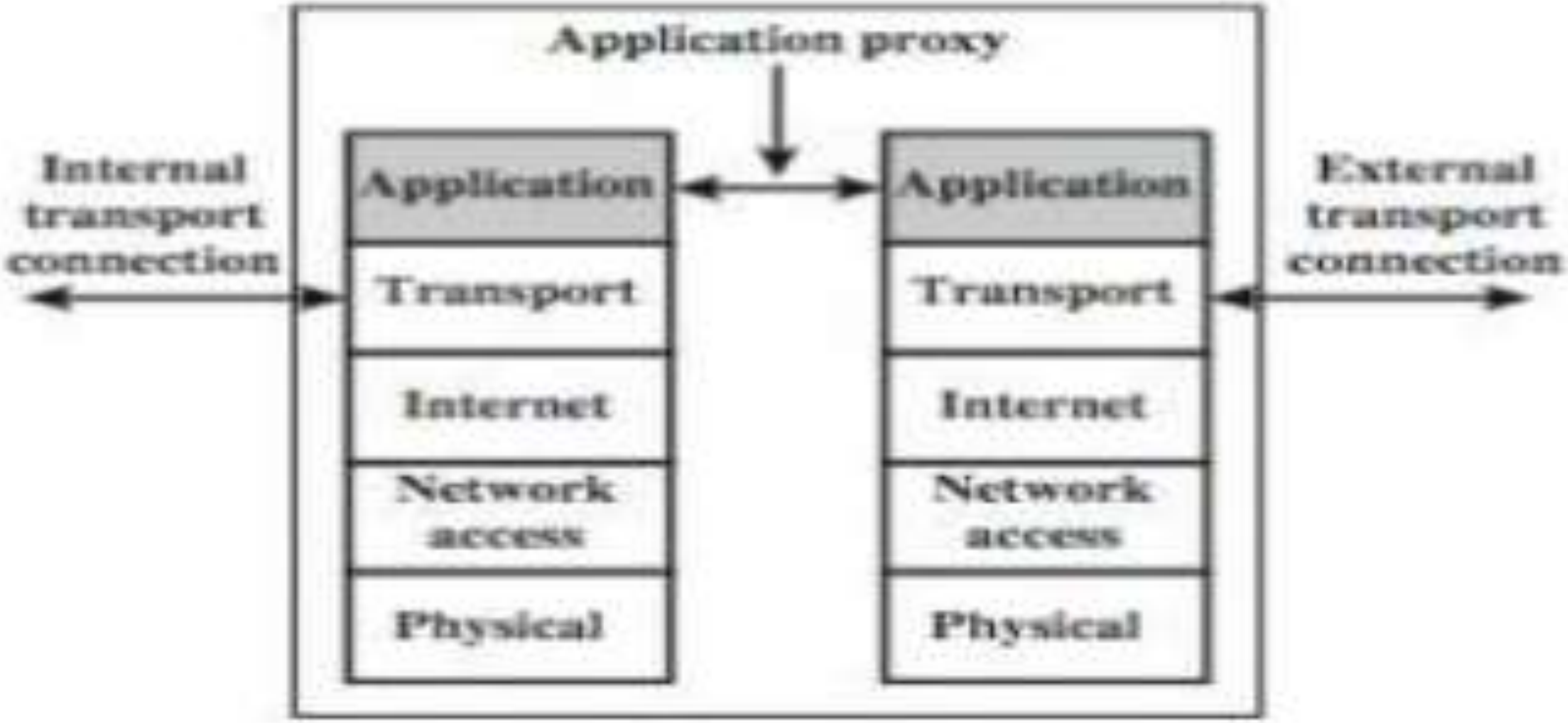
- **Disdavnteges:**

✓ Can work only on the network layer

✓ Do not support complex rule based support

✓ Vulnerable to spoofing

# Application Proxy Firewall



# Application Proxy Firewall

- An application –level also cal an application proxy, acts as a rely of application-level traffic.
- User request service from proxy
- Proxy validates request as legal
- Then actios request and returns result to user
- Can log/and traffic at applicationl lev

# Application Proxy Firewall

- **Advantages:**
  - ✓ More secure than packet filter firewalls
  - ✓ Easy to log and audit incoming traffic
- **Disadvatages:**
  - ✓ Additional processing overhead on each connection

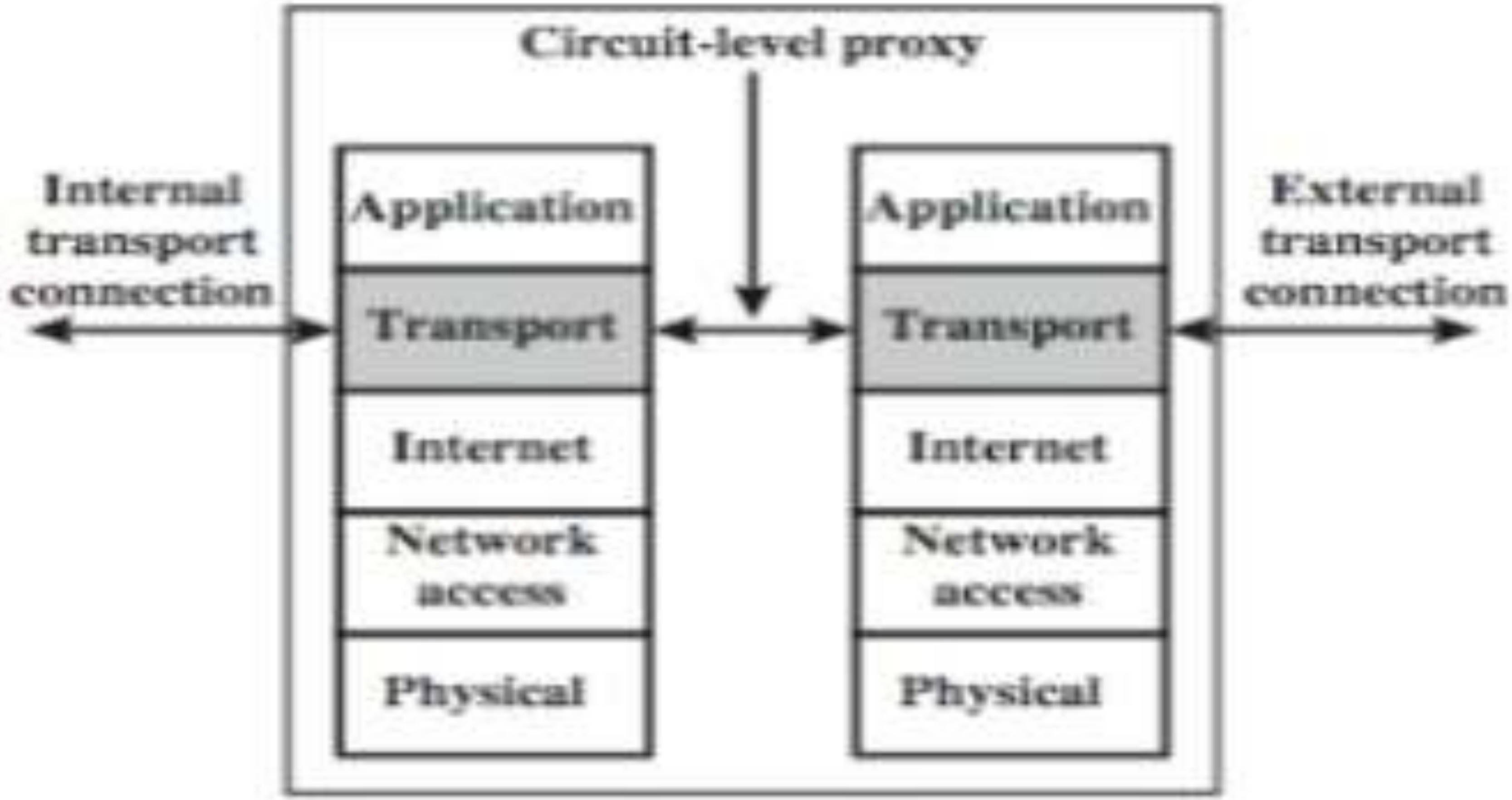
# Stateful Inspection Firewall

- A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections.
- There is an entry for each currently established connections.
- The packet filter now allow incoming traffic to high- numbered ports only for those packets that fit the profit of one of the entries in this directory.
- A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections.

# Stateful Inspection Firewall

- **Advantages:**
  - ✓ Can work on a transparent mode allowing direct connections between the client and the server.
  - ✓ Can also implement algorithms and complex security modls which are protocol specific, making the connections and data transfer more secure.

# Circuit – level Firewall



# Circuit-level Firewall

- This can be a stand-alone system or it can be a specialized functions performed by an application- level gateway for certain applications
- It does not permit an end-to-end TCP connections, rather the gateway sets two TCP connections.
- A typical use of the circuit-level gateway is a situation in which the system administer trusts the internal users.
- The gateway can be configured to support application –level or proxy service on inbound connections and circuit-level functions for outbound connections.

# Circuit-level Firewall

- **Advantages:**
  - ✓ Comparatively inexpensive and provide Anonymity to the private network.
- **Disadvantages**
  - ✓ Do not filter individual packets

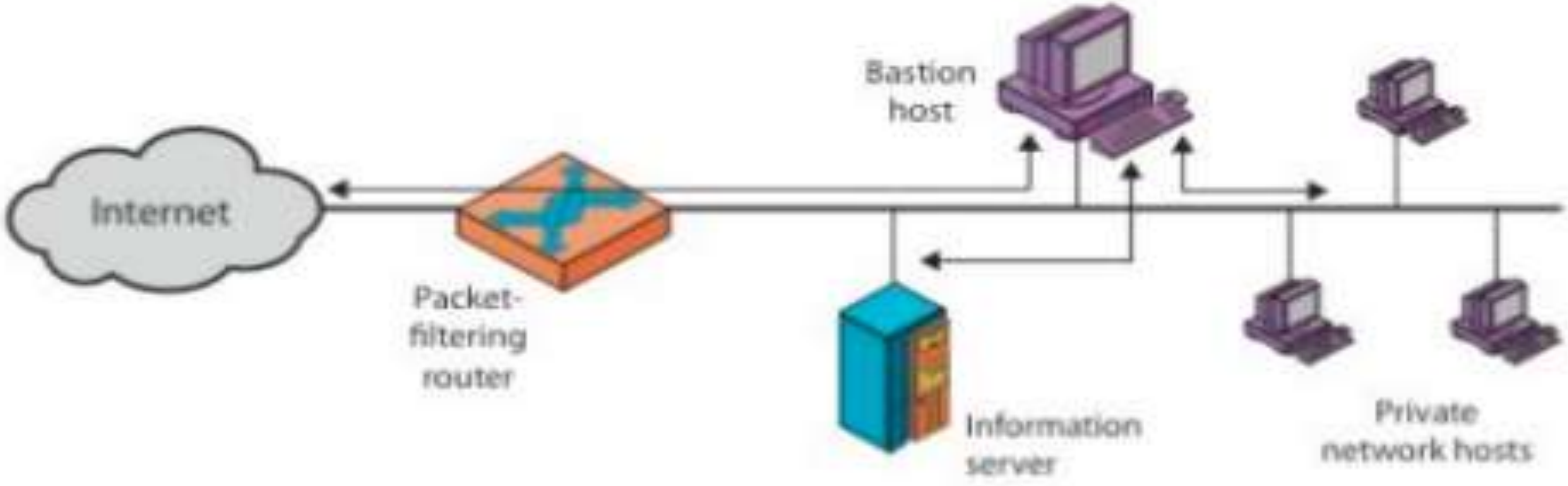
# Firewall Configuration

- **In addition to the use of simple configuration of a single system( single packet filtering router or single gateway), more complex configurations are possible.**
  - ✓ Screened host firewall system(single-homed bastion host)
  - ✓ Screened host firewall system (dual-homed bastion host)
  - ✓ Screened-sunbet firewall system

# Screened host firewall system (single-homed bastion host

- **Firewall consists of two system:**
  - ✓ A packet-filtering router
  - ✓ A bastion host
- **The router is configured so that**
  - ✓ For traffic from internet, only IP packet destined for the bastion host are allowed in.
  - ✓ For traffic from the internal network only IP packets from the bastion host are allowed out.
- **The bastion host performs authentication and proxy functions**.

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

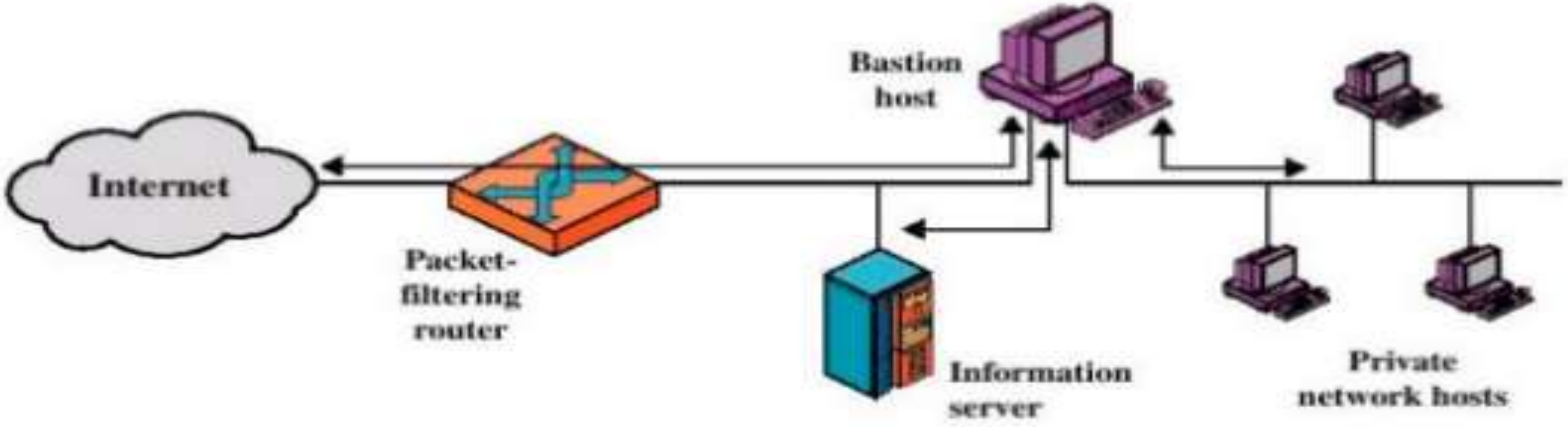


(a) Screened host firewall system (single-homed bastion host)

# Screened host firewall, dual-homed bastion configuration

- The packet-filtering router is not completely compromised.
- Traffic between the Internet and other hosts on the private has to flow through the bastion host.

# Screened host firewall, dual-homed bastion configuration

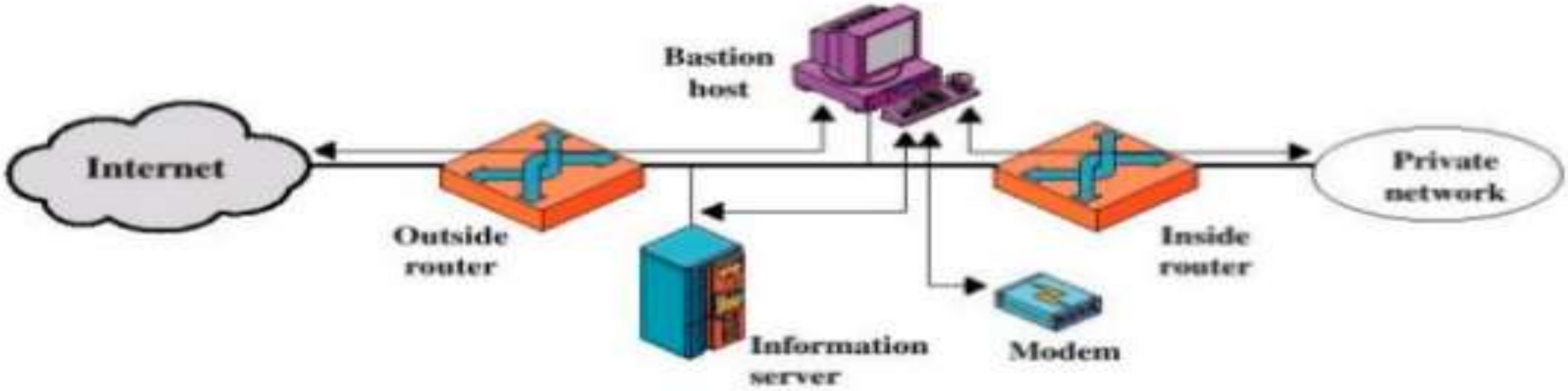


# Screened subnet firewall configuration

- **Most secure configuration of the three**
- **Two packet-filtering routers are used**
- **Creation of an isolated sub-network.**

  - which consists of simply the bastion host, may also include one or more information servers and modems.

# Screened subnet firewall configuration



# Firewall Limitation

- Cannot protect from attacks bypassing it

  - example sneaker net, utility modems, trusted organisations, trusted services(eg SSl/SSH)
- Cannot protect against internal threats

  - example disgruntled or colluding employees
- Cannot protect against access via WLAN

  - if improperly secured against external use
- Cannot protect against malware imported via laptop, storage infected outside

# Thank You