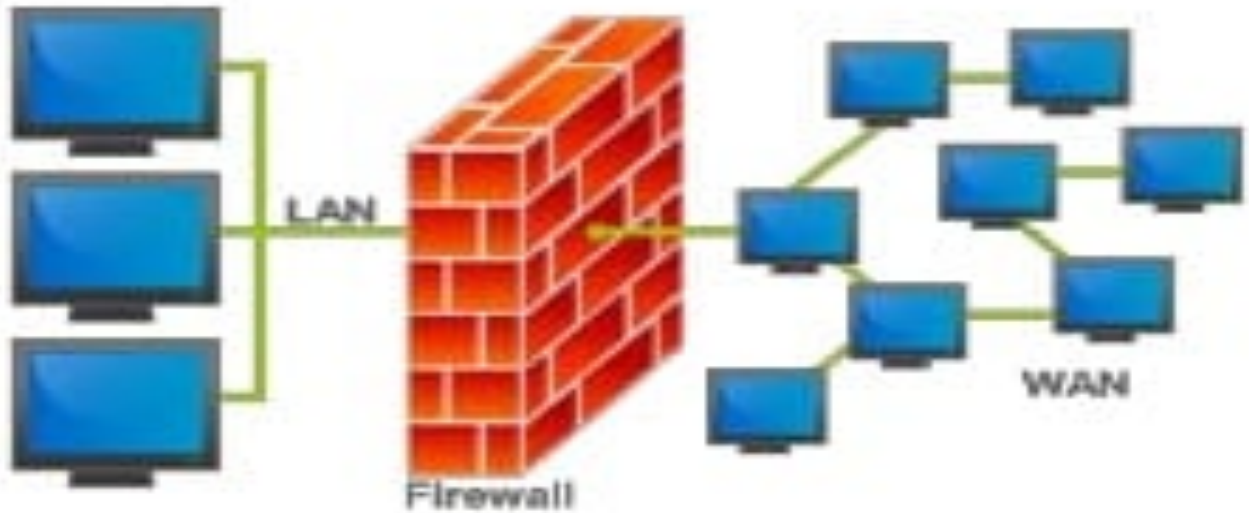
Firewalls

Outline

- Firewall Design Principles
  - Firewall Characteristics
  - Types of Firewalls
  - Firewall Configurations
- Trusted Systems
  - Data Access Control
  - The Concept of Trusted systems
  - Trojan Horse Defense

Firewalls

- Effective means of protection a local system or network of systems from network-based security threats while affording access to the outside world via WAN`s or the Internet



Firewall Design Principles

- Information systems undergo a steady evolution (from small LAN`s to Internet connectivity)
- Strong security features for all workstations and servers not established

Firewall Design Principles

- The firewall is inserted between the premises network and the Internet
- Aims:
  - Establish a controlled link
  - Protect the premises network from Internet-based attacks
  - Provide a single choke point

Firewall Characteristics

- Design goals:
  - All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
  - Only authorized traffic (defined by the local security policy) will be allowed to pass

Firewall Characteristics

- Design goals:
  - The firewall itself is immune to penetration (use of trusted system with a secure operating system)

Firewall Characteristics

- Four general techniques:
- Service control
  - Determines the types of Internet services that can be accessed, inbound or outbound
- Direction control
  - Determines the direction in which particular service requests are allowed to flow

Firewall Characteristics

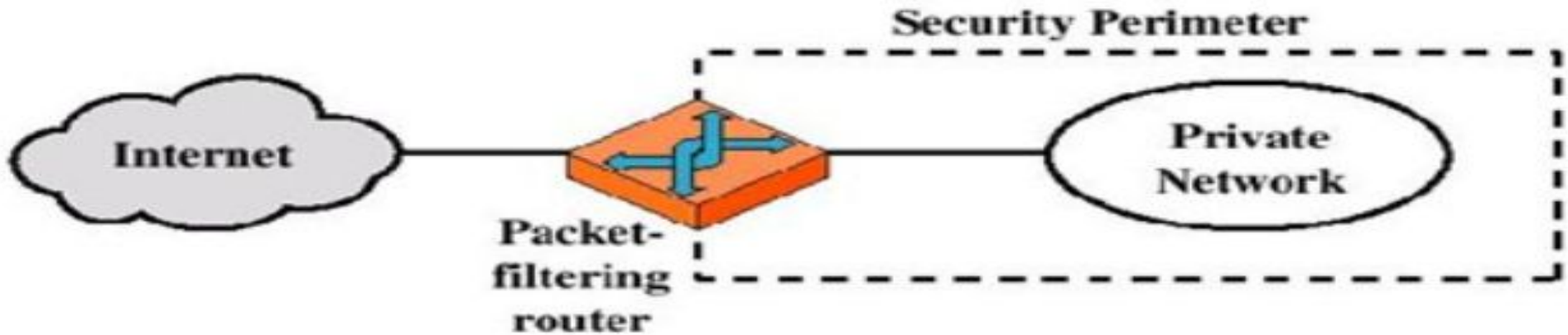
- User control
  - Controls access to a service according to which user is attempting to access it
- Behavior control
  - Controls how particular services are used (e.g. filter e-mail)

Types of Firewalls

- Three common types of Firewalls:
  - Packet-filtering routers
  - Application-level gateways
  - Circuit-level gateways
  - (Bastion host)

Types of Firewalls

- Packet-filtering Router



Types of Firewalls

- Packet-filtering Router
  - Applies a set of rules to each incoming IP packet and then forwards or discards the packet
  - Filter packets going 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
  - Two default policies (discard or forward)

Types of Firewalls

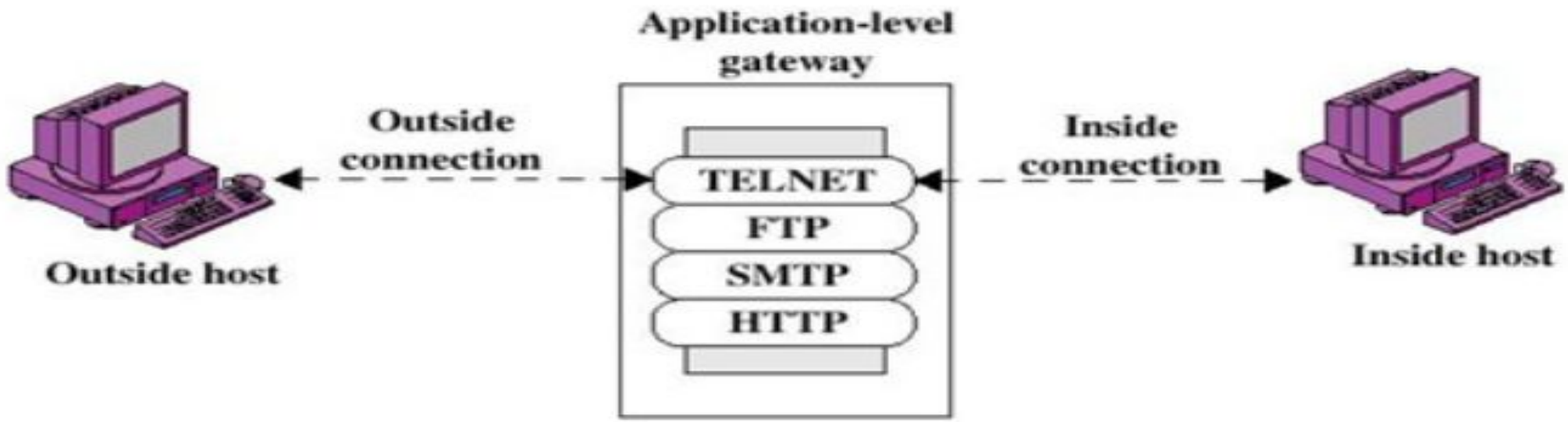
- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication

Types of Firewalls

- Possible attacks and appropriate countermeasures
  - IP address spoofing
  - Source routing attacks
  - Tiny fragment attacks

Types of Firewalls

- Application-level Gateway



Types of Firewalls

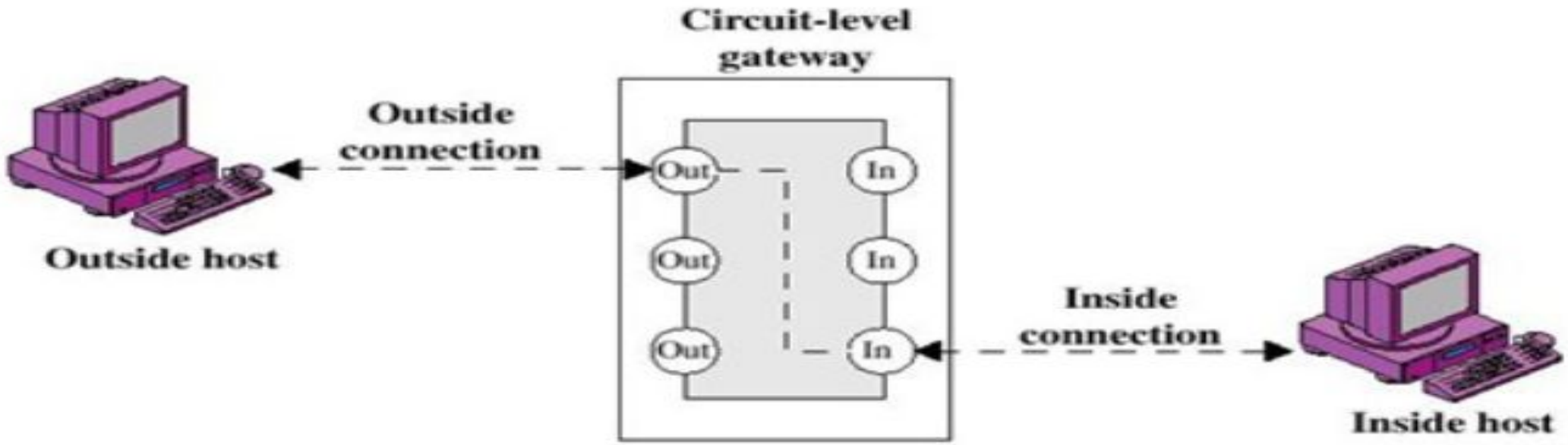
- Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic

Types of Firewalls

- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)

Types of Firewalls

- Circuit-level Gateway



Types of Firewalls

- Circuit-level Gateway
  - Stand-alone system or
  - Specialized function performed by an Application-level Gateway
  - Sets up two TCP connections
  - The gateway typically relays TCP segments from one connection to the other without examining the contents

Types of Firewalls

- Circuit-level Gateway
  - The security function consists of determining which connections will be allowed
  - Typically use is a situation in which the system administrator trusts the internal users
  - An example is the SOCKS package

Types of Firewalls

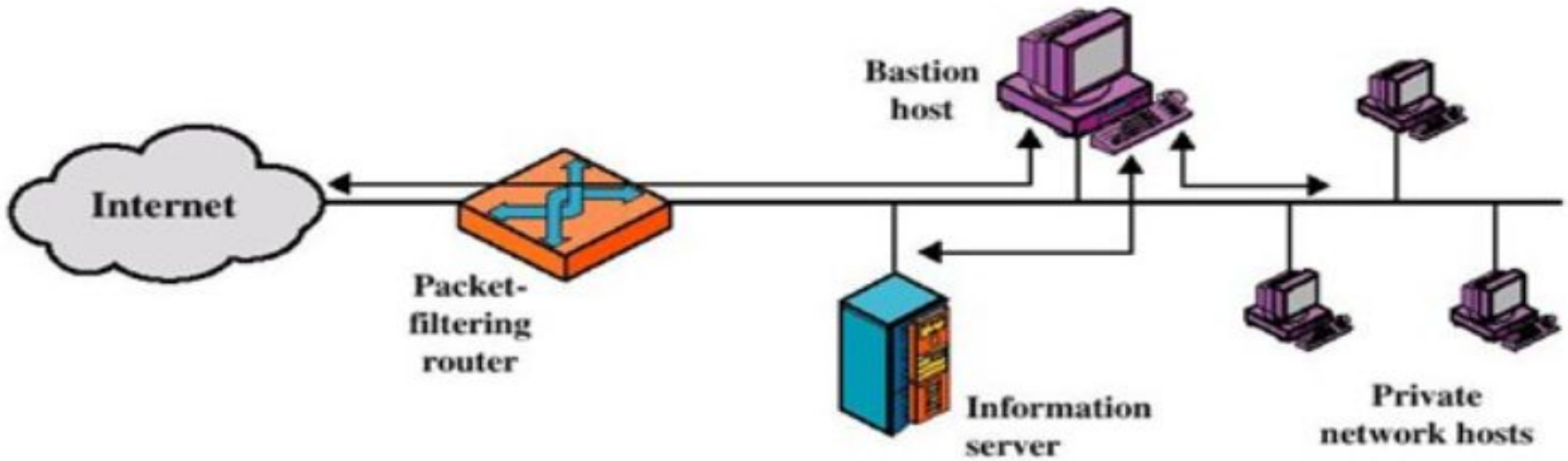
- Bastion Host
  - A system identified by the firewall administrator as a critical strong point in the network´s security
  - The bastion host serves as a platform for an application-level or circuit-level gateway

Firewall Configurations

- In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible
- Three common configurations

Firewall Configurations

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



Firewall Configurations

- Screened host firewall, single-homed bastion configuration
- Firewall consists of two systems:
  - A packet-filtering router
  - A bastion host

Firewall Configurations

- Configuration for the packet-filtering router:
  - Only packets from and to the bastion host are allowed to pass through the router
- The bastion host performs authentication and proxy functions

Firewall Configurations

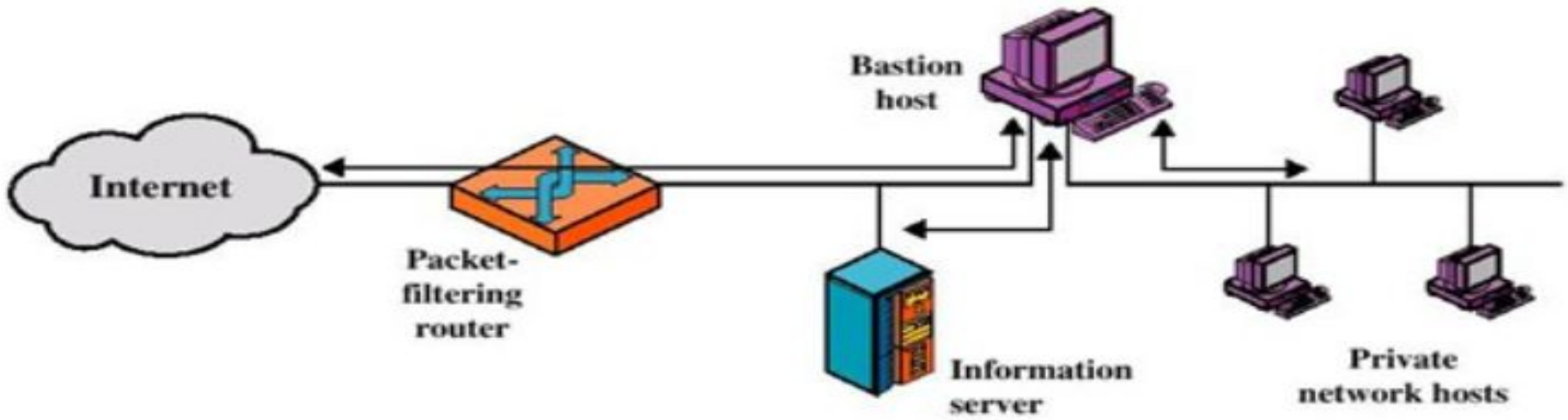
- Greater security than single configurations because of two reasons:
  - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
  - An intruder must generally penetrate two separate systems

Firewall Configurations

- This configuration also affords flexibility in providing direct Internet access (public information server, e.g. Web server)

Firewall Configurations

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

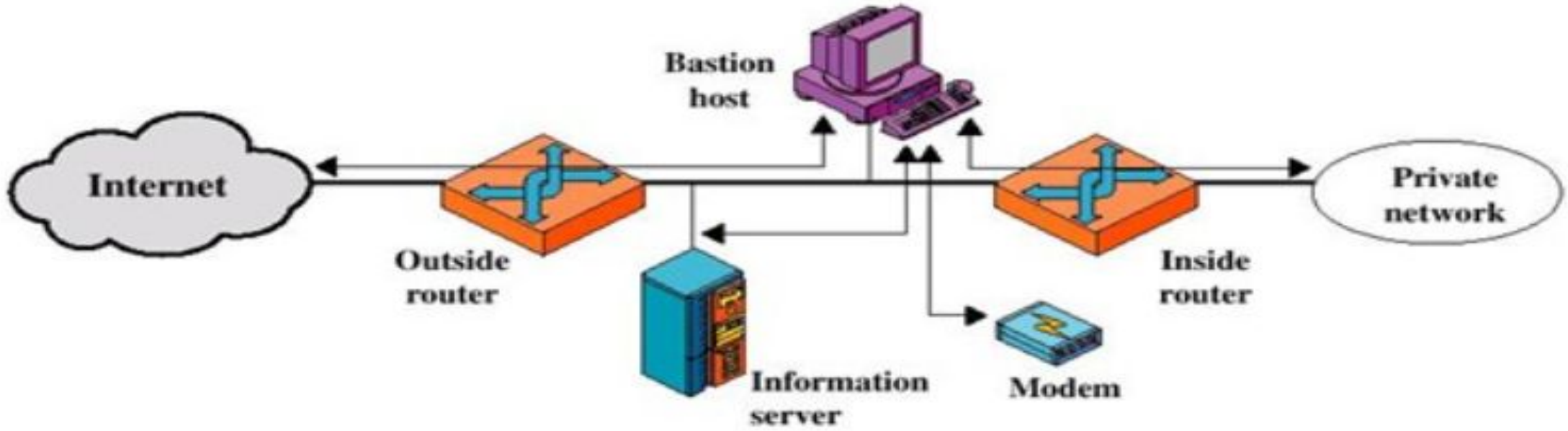


Firewall Configurations

- 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 network has to flow through the bastion host

Firewall Configurations

- Screened-subnet firewall system



Firewall Configurations

- Screened subnet firewall configuration
  - Most secure configuration of the three
  - Two packet-filtering routers are used
  - Creation of an isolated sub-network

Firewall Configurations

- Advantages:
  - Three levels of defense to thwart intruders
  - The outside router advertises only the existence of the screened subnet to the Internet (internal network is invisible to the Internet)

Firewall Configurations

- Advantages:
  - The inside router advertises only the existence of the screened subnet to the internal network (the systems on the inside network cannot construct direct routes to the Internet)

Trusted Systems

- One way to enhance the ability of a system to defend against intruders and malicious programs is to implement trusted system technology