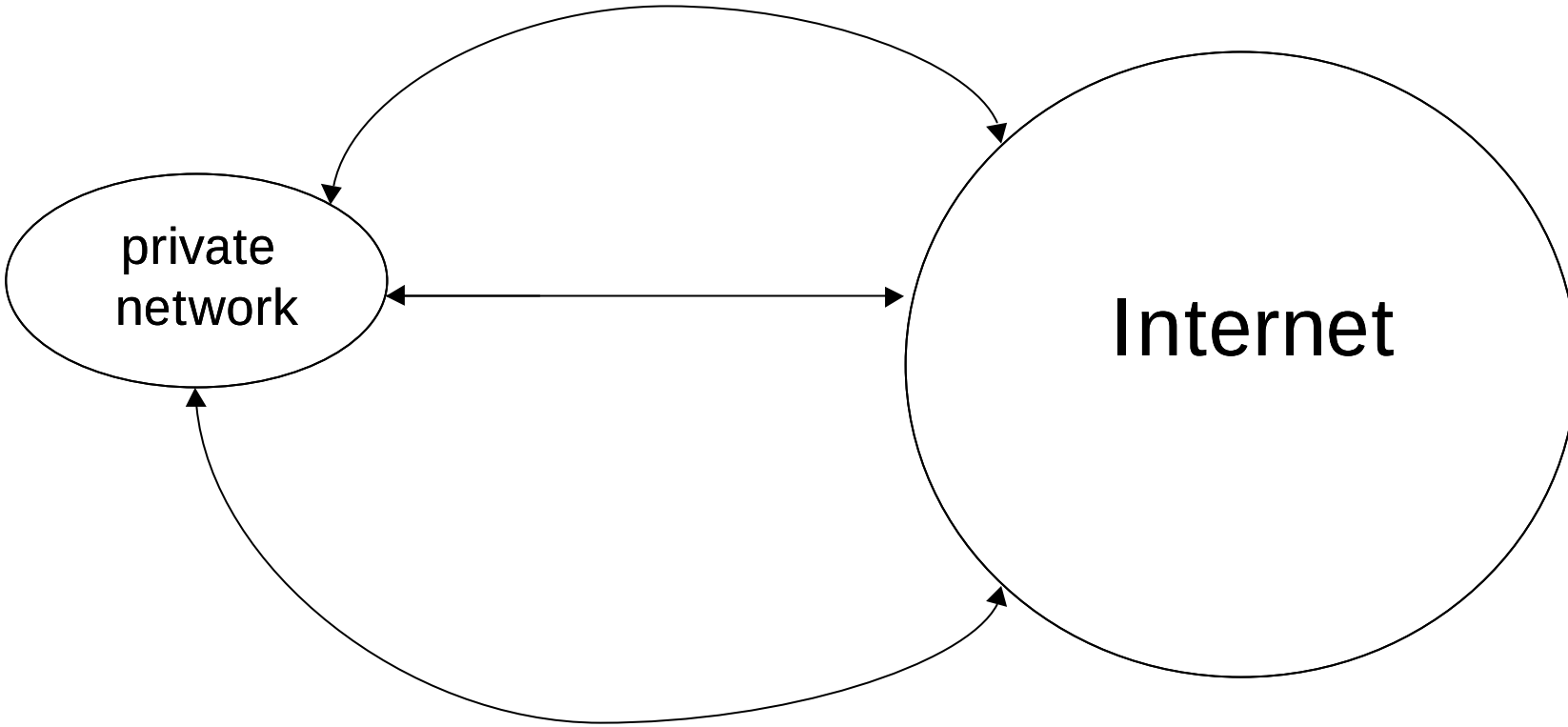
Firewalls

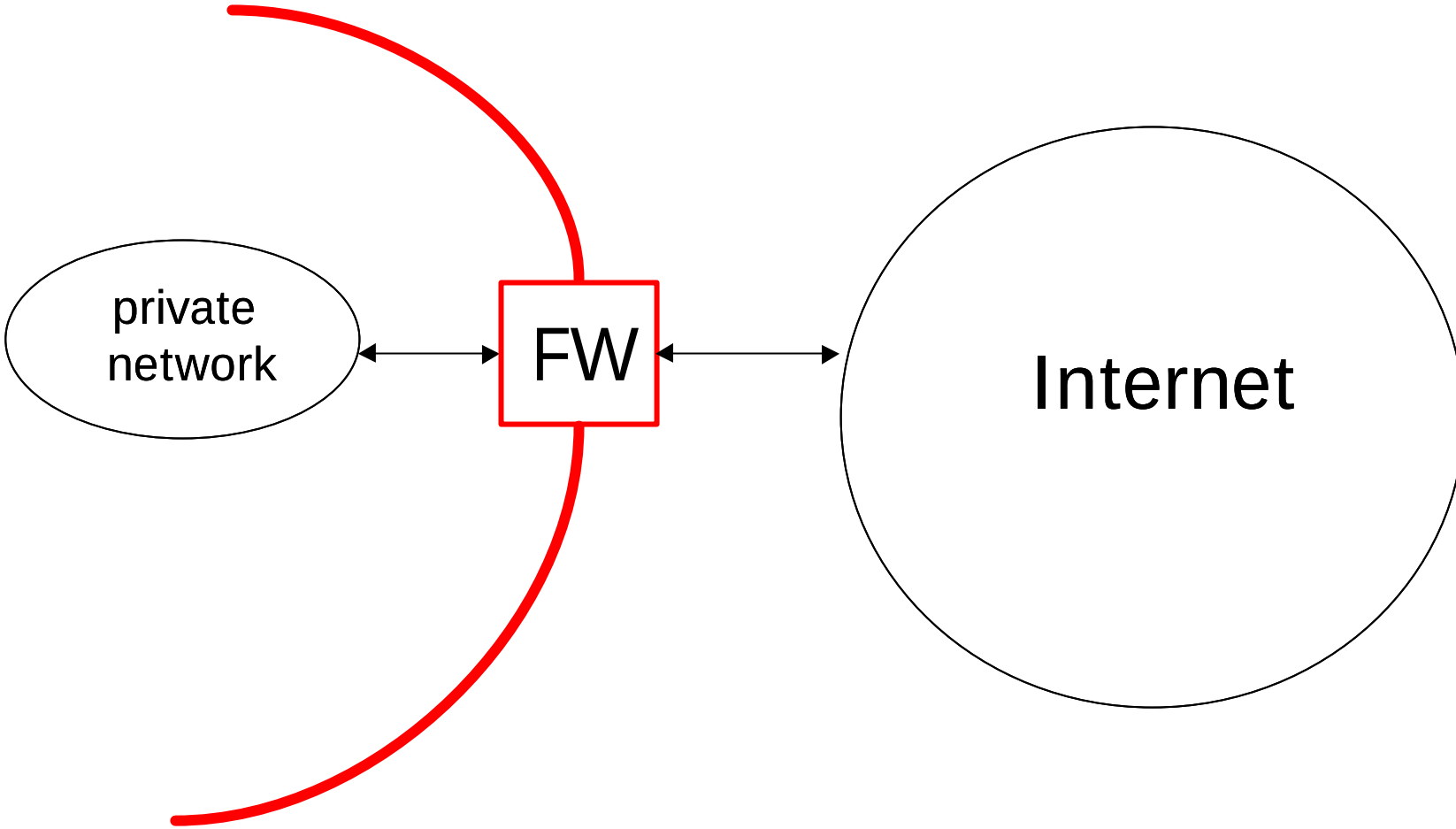
Firewall

- It’s a network component used to
  - Protect a private network from external malicious or unauthorised access and provide external connectivity at the same time
  - Easily manage in a centralised fashion the security of a network
  - Protection against outsiders

Firewall



Firewall



Firewalls

- 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

Firewalls

- Design goals:

  – The firewall itself is immune to penetration (use of trusted system with a secure operating system)

Firewalls

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

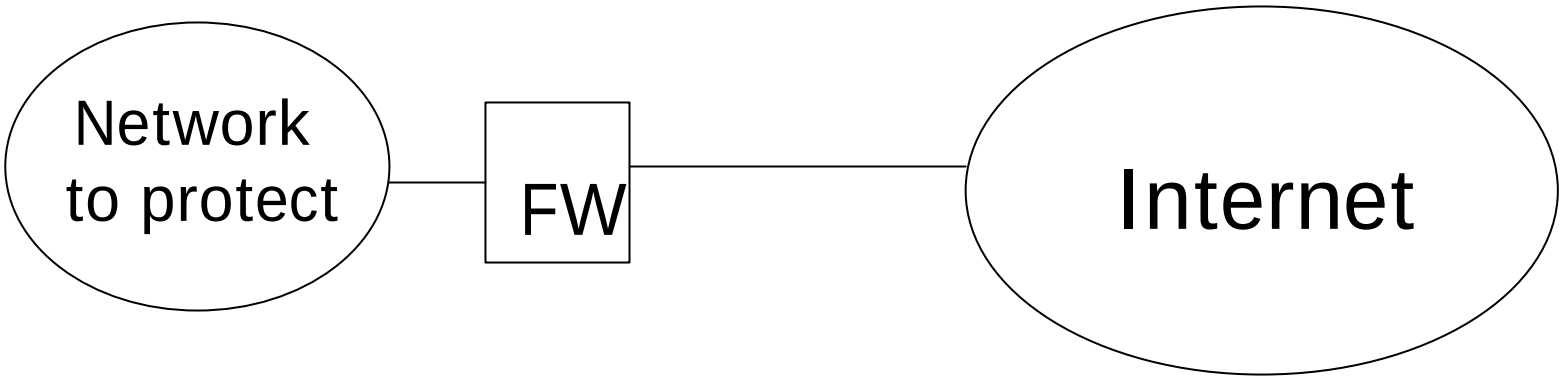
Firewalls

- 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 spam e-mail)

Firewalls

- Three common types:
  - Packet-filtering routers
  - Application-level gateways
  - Circuit-level gateways

Packet Filtering



Packet Filtering

- Applies a set of rules to each *incoming IP packet* to decide whether it should be forwarded or discarded.

- *Header information* is used for filtering (e.g, protocol number, source and destination IP, source and destination port numbers, etc.)

- *Stateless*: each IP packet is examined isolated from what has happened in the past.

- Often *implemented* by a router

Packet Filtering

Example of policies

A

action	ourhost	port	theirhost	port	comment
block	*	*	digot	*	**We don't trust these**
allow	Our-GW	25	*	*	**Connection to our SMTP port**

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	**deault**

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	**Connection to their SMTP port**

Packet Filtering

Example of policies

action	src	port	dest	port	flags	comment
allow	{our-host}	*	*	25		**Our packets to their SMTP port**
allow	*	25	*	*	ACK	**Their replies**

action	src	port	dest	port	flags	comment
allow	{our-host}	*	*	*		**Our outgoing calls**
allow	*	*	*	*	ACK	**Replies to our calls**
allow	*	*	*	>1024		**Traffic to non servers**

Packet Filtering: Pros

- Transparent. It does not change the traffic flow or characteristics –passes it through or doesn't
- Simple
- Cheap
- Flexible: filtering is based on current rules

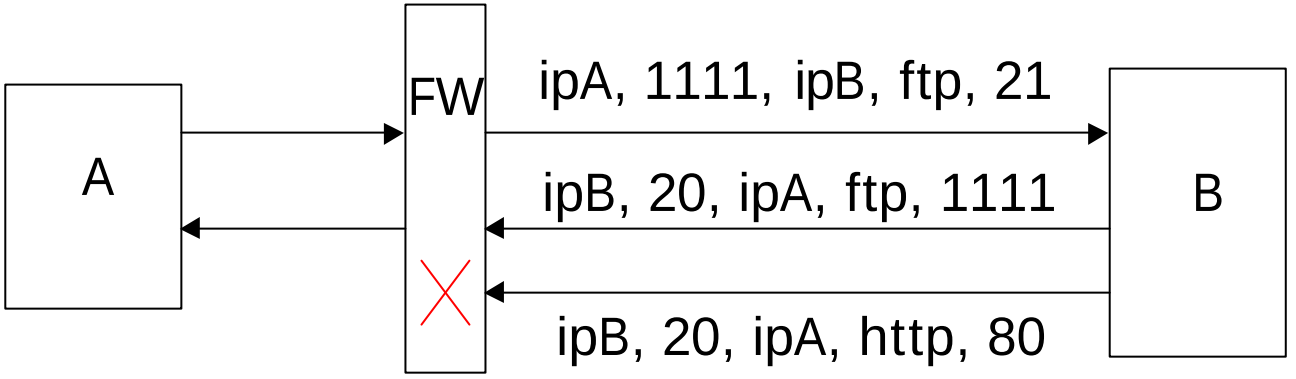
Packet Filtering: Cons

- It does not filter application-specific attacks
- Unsophisticated (protects against simple attacks)
- Calibrating rule set may be tricky
- Limited auditing
- Single point of failure

Stateful Packet Filtering

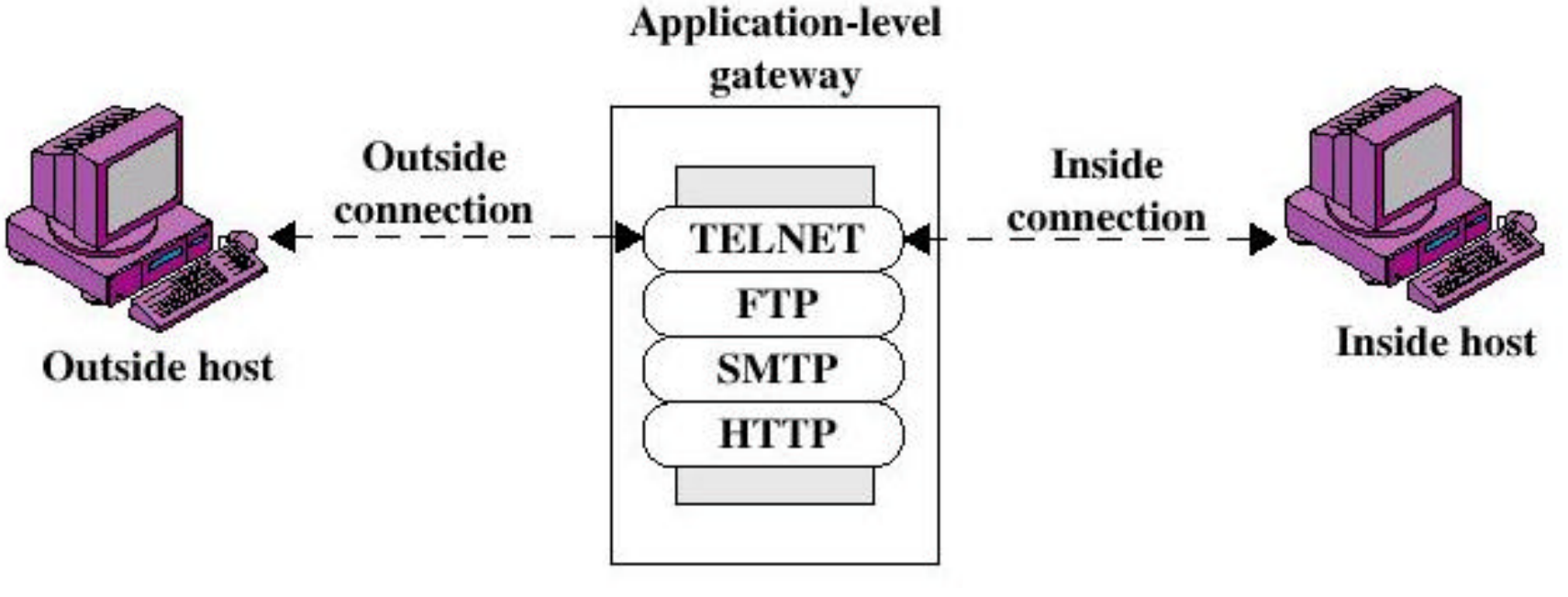
- Called *Stateful Inspection* or *Dynamic Packet Filtering*

- Maintains a history of *previously seen packets* to make better decisions about current and future packets



Application Level Gateway

– Also called proxy server
– Acts as a relay of application-level traffic
– All connections are mediated by the GW



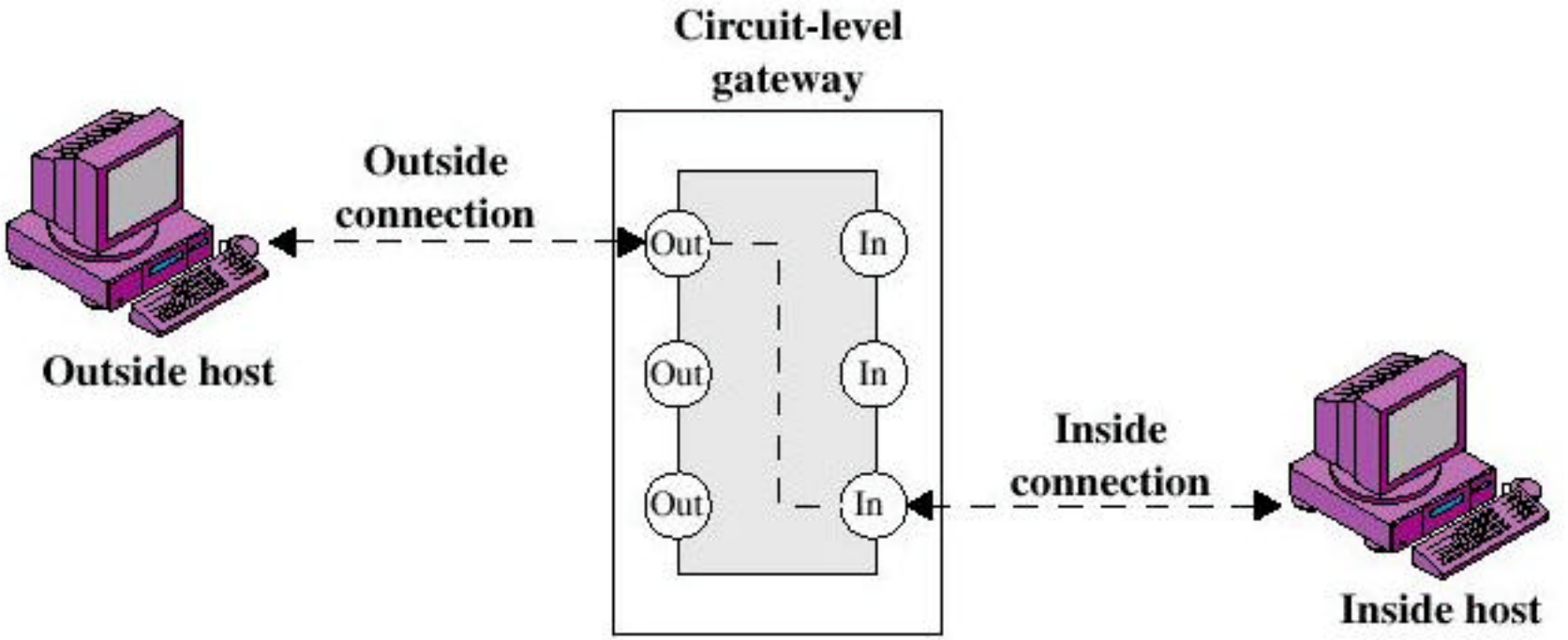
Application Gateway: Pros

- Advantages: by not permitting application traffic directly to internal hosts
  - *Information hiding*: names of internal systems are not known to outside systems
  - Can limit capabilities within an application
  - *Robust authentication and logging*: application traffic can be pre-authenticated before reaching host and can be logged
  - *Cost effective*: third-party software and hardware for authentication and logging only on gateway
  - *Less-complex filtering rules for packet filtering routers*: need to check only destination
  - More secure

Application Gateway: Cons

- Keeping up with new applications
- Need to know all aspects of protocols
- May need to modify application client/protocols

Circuit-level Gateway



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

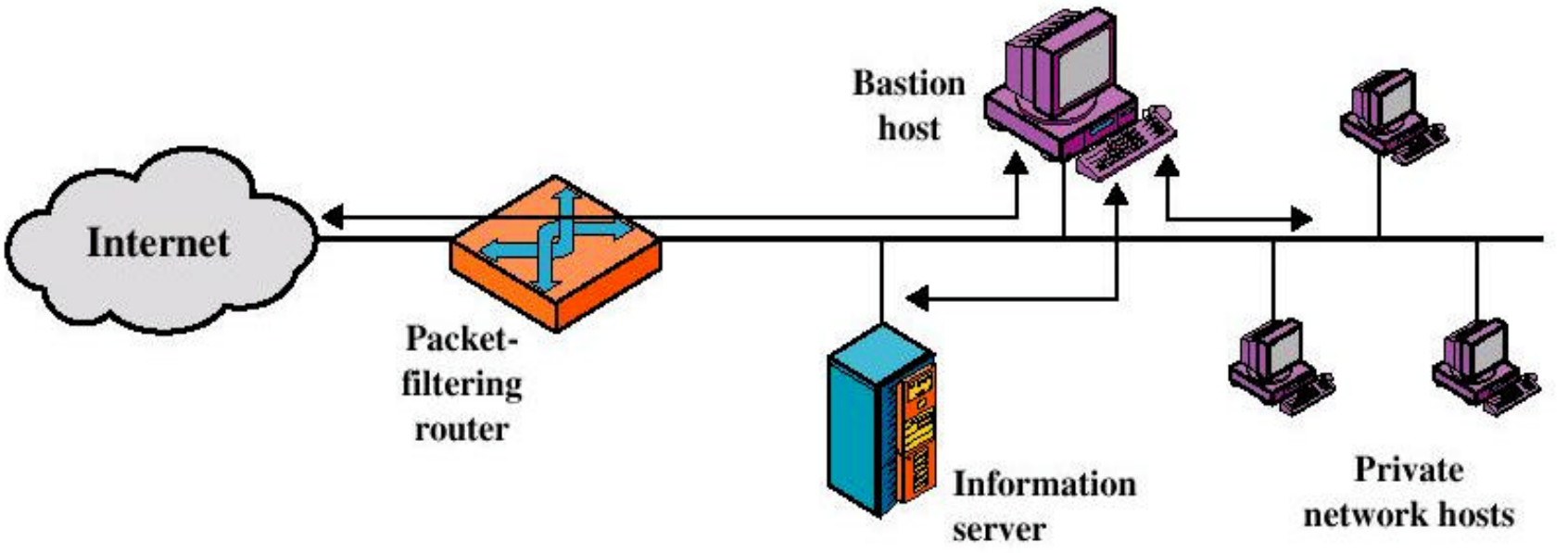
Bastion Host

– 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

- 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

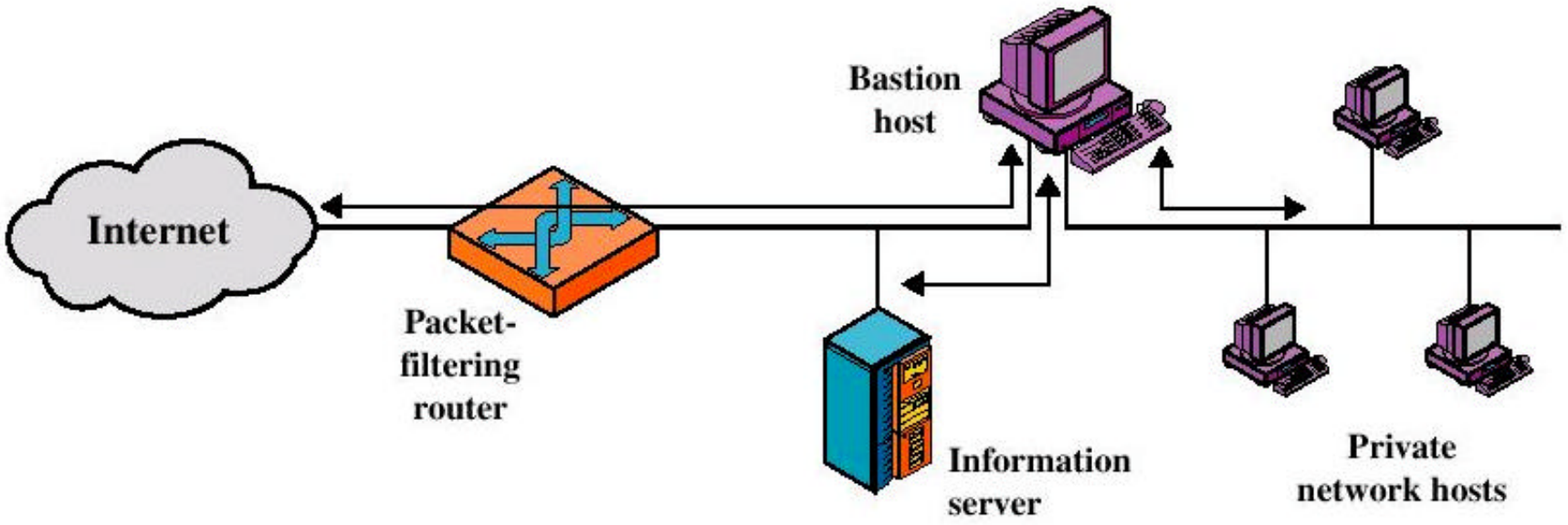
- Greater security than single configurations because of two reasons:
  - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
  - An intruder must generally penetrate two separate systems

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)

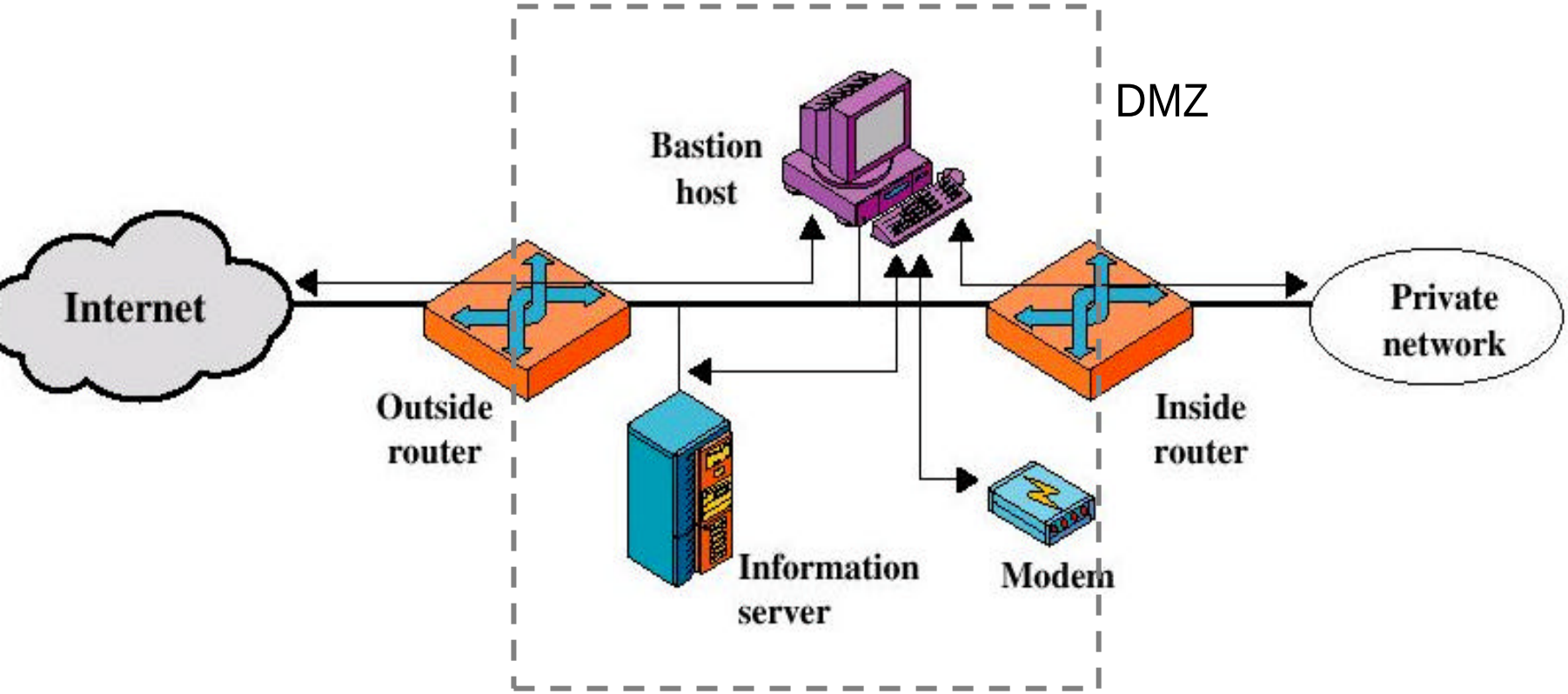


Firewall Configurations

- Screened host firewall, dual-homed bastion configuration
  - If the packet-filtering router is completely compromised the private network is still protected
  - Traffic between the Internet and other hosts on the private network has to physically 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 (DMZ)

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)