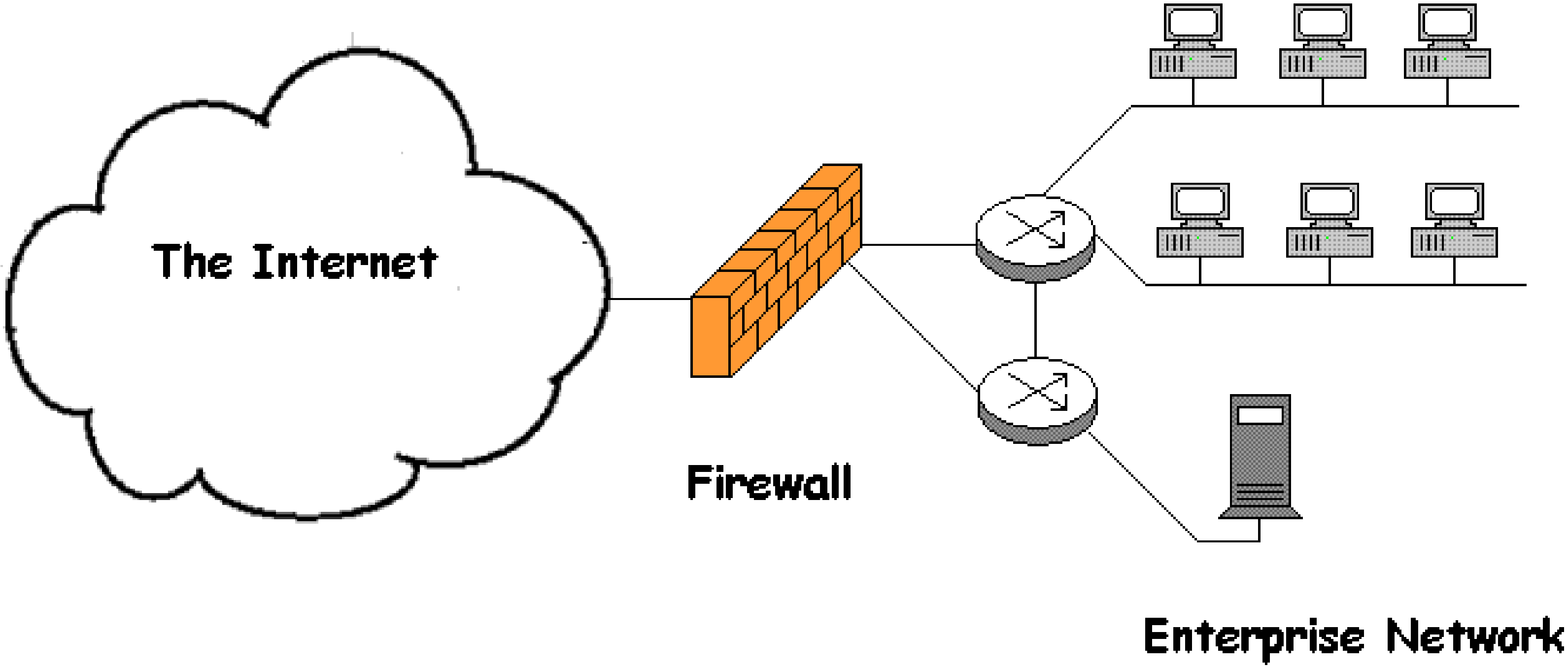
Firewall

Firewalls -Introduction

- A firewall is a way of restricting access to a LAN or a portion of a LAN.
- Firewalls are concerned with the Security Goal of Access Control

Firewalls and the Internet



Connectivity to the internet is an essential feature for the computer systems of all modern enterprises. All traffic passing between the enterprise network and the internet passes through the firewall. The firewall is the choke point at which security and auditing can be imposed.
The firewall hardware can consist of one or more PCs, routers or other specialised hardware devices.

Firewall Design Goals

- All traffic coming from or going to, the internet must pass through the firewall.
- Only authorized traffic, as defined by the local security policy can pass through the firewall.
- The firewall itself is immune to penetration. The firewall itself is a trusted system.

Firewall –Controls

- 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
- 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)

Essential and Convenient Firewall Capabilities

Essential Capabilities

- A single choke point for management of a network’s connection to the internet.
- A location for monitoring and logging security related events.

Other capabilities

- Network Address Translation (NAT)
- IPSec **tunnel** mode station (the other is transport mode)

Firewall Limitations

- Cannot protect against attacks that bypass the firewall e.g. dial in modems on internal LAN
- Cannot protect against internal attacks e.g. a disgruntled employee.
- Cannot protect against the transfer of viruses. In most cases it is either impractical or impossible to scan all data and files transferred in.

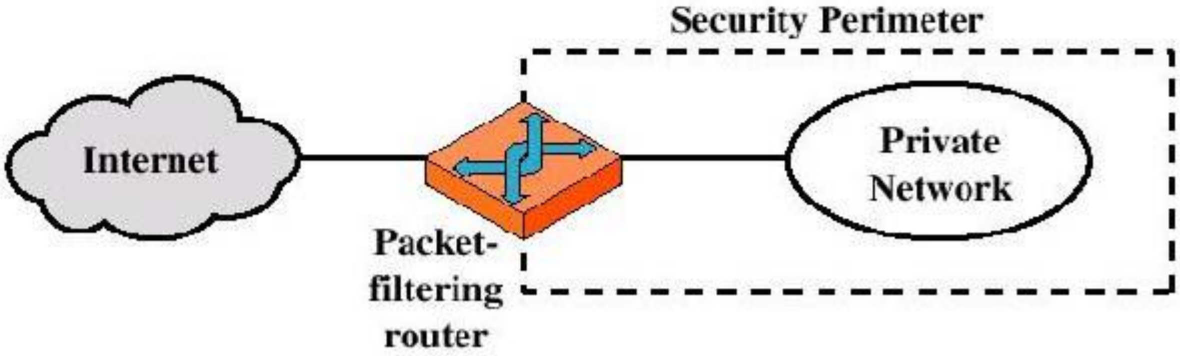
Types of Firewalls

Three common types of firewalls:

- Packet-filtering firewall
  - This is the most common type of firewall
- Circuit-level gateway
  - Work at the session level of the OSI Network Layer Model
- Application-level gateway
  - Often used in conjunction with a packet filtering firewall

Types of Firewalls

- Packet-filtering Router



Packet-filtering Router

- 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)

Firewall Filtering

Typically filter packets on following criteria – criteria can usually be compounded together:

- IP address of source or destination
- Port Number of source or destination
- Hardware Interface
- Packet Type –tcp, udp, icmp
- Packet characteristics e.g. flag

Packet Filter Firewall Advantages and Disadvantages

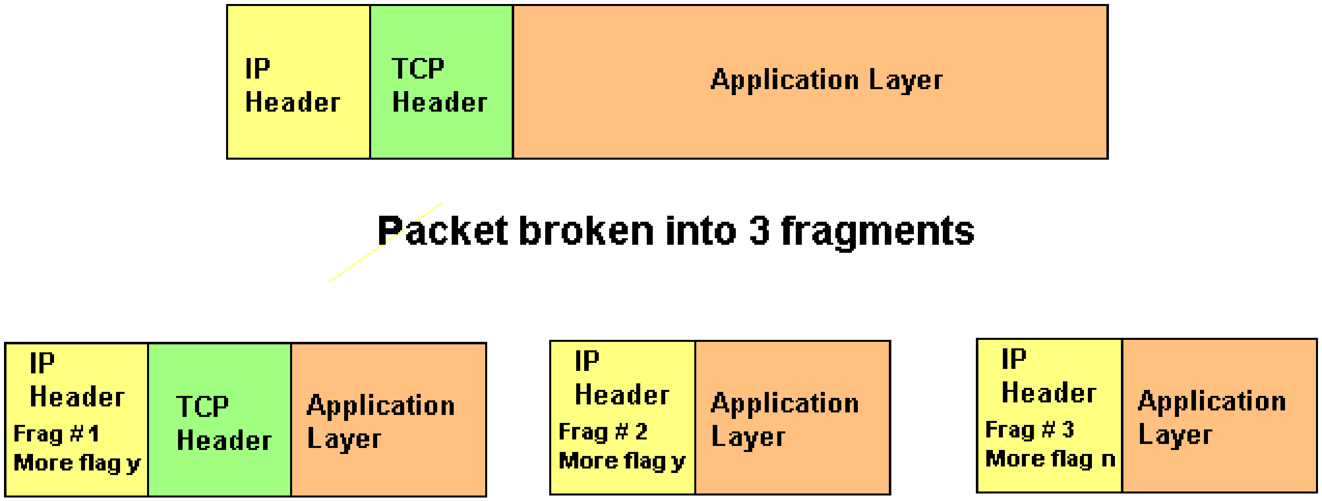
- Advantages:
  - Simplicity
  - Transparency to users
  - High speed

- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication
  - Can slow down network speed if there are a lot of rules. **(many if statements!)**

Some possible packet firewall attacks and appropriate countermeasures

- IP address spoofing. These can be prevented through correct configuration.
- Fragmentation attacks. All fragmented packets should be denied. (see next slide)

Packet Fragmentation



IP Header | TCP Header | Application Layer

Packet broken into 3 fragments

IP Header Frag # 1 More flag y | TCP Header | Application Layer

IP Header Frag # 2 More flag y | Application Layer

IP Header Frag # 3 More flag n | Application Layer

Only the first fragment has a TCP header

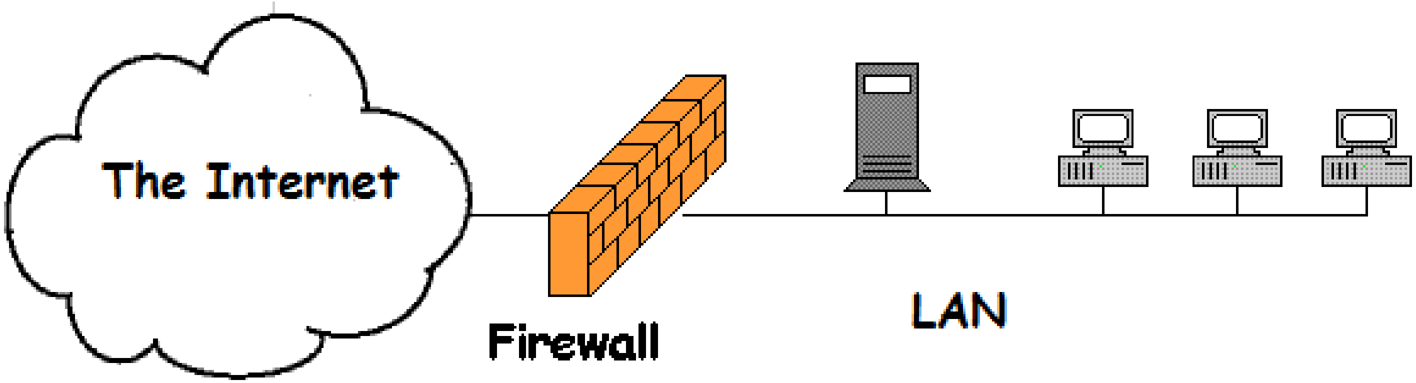
Packets may travel through many different devices before reaching their final destination. Some transmission media have small maximum packet sizes and they will break large packets into fragments. The diagram above shows how fragmentation occurs. Each fragment has a fragment number and a "more" flag in the IP header. The first fragment has a TCP header, but following fragments do not.
As a result of this, firewalls have problems matching fragmented packets with firewall rules. In addition, attackers can send large numbers of fragments except the first, as a DOS attack or as a way of defeating the firewall.

Firewalls should deny all fragmented packets.

Packet Firewall Configurations

- Packet filtering firewalls are usually set up by a configuration file. The script allows and restricts access. There are two types of firewall script design.
  - Exclusive: An exclusive firewall allows all traffic through except for the traffic matching the ruleset.
  - Inclusive: only allows traffic matching the rules through and blocks everything else.

Firewall Configuration Inclusive Type



Inclusive Firewall Configuration :

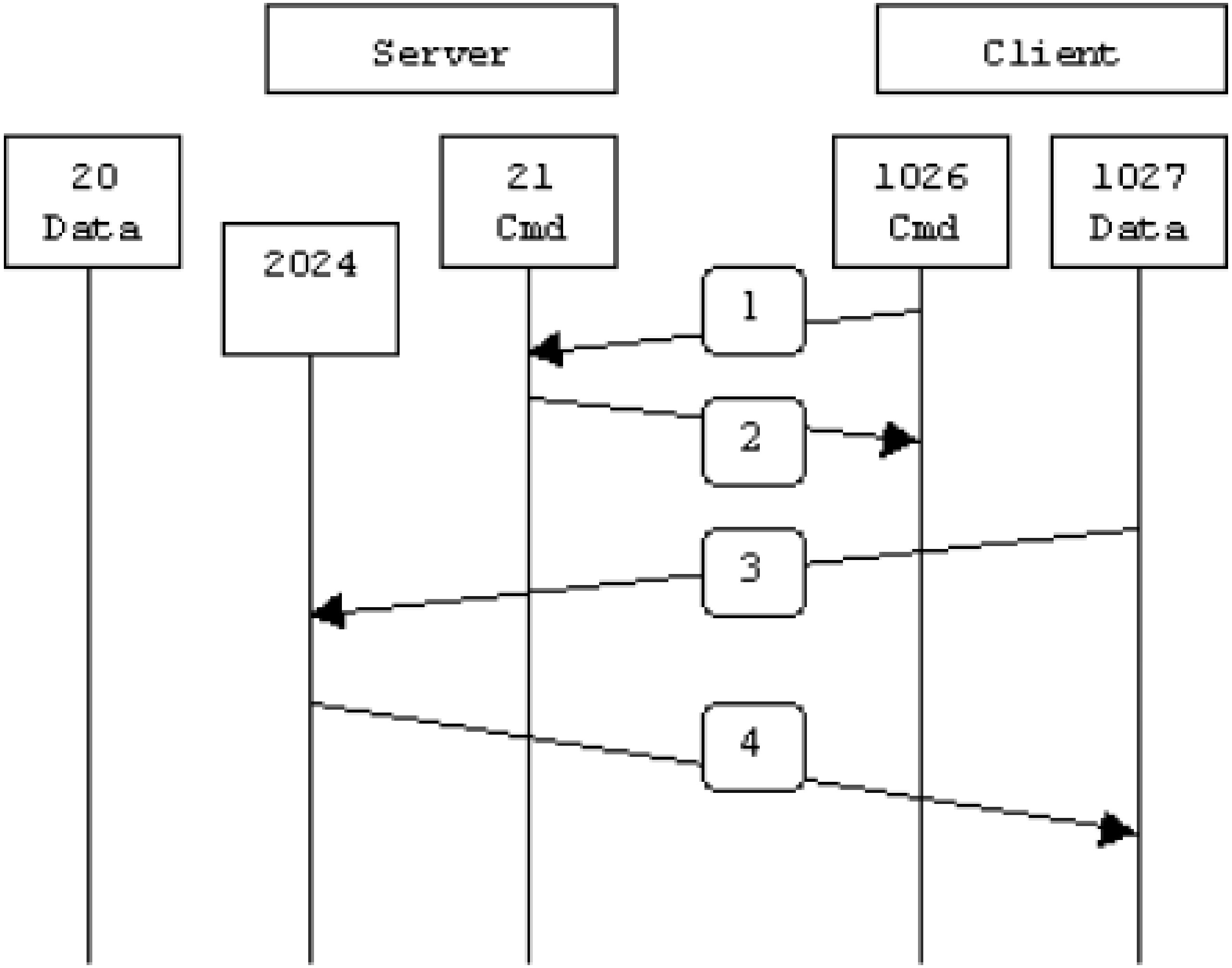
All traffic in both directions is blocked. Then specific types of traffic in either direction are allowed.

Inclusive firewall configurations are harder to write than exclusive configurations, but they are much more secure. Exclusive firewall types are very insecure.

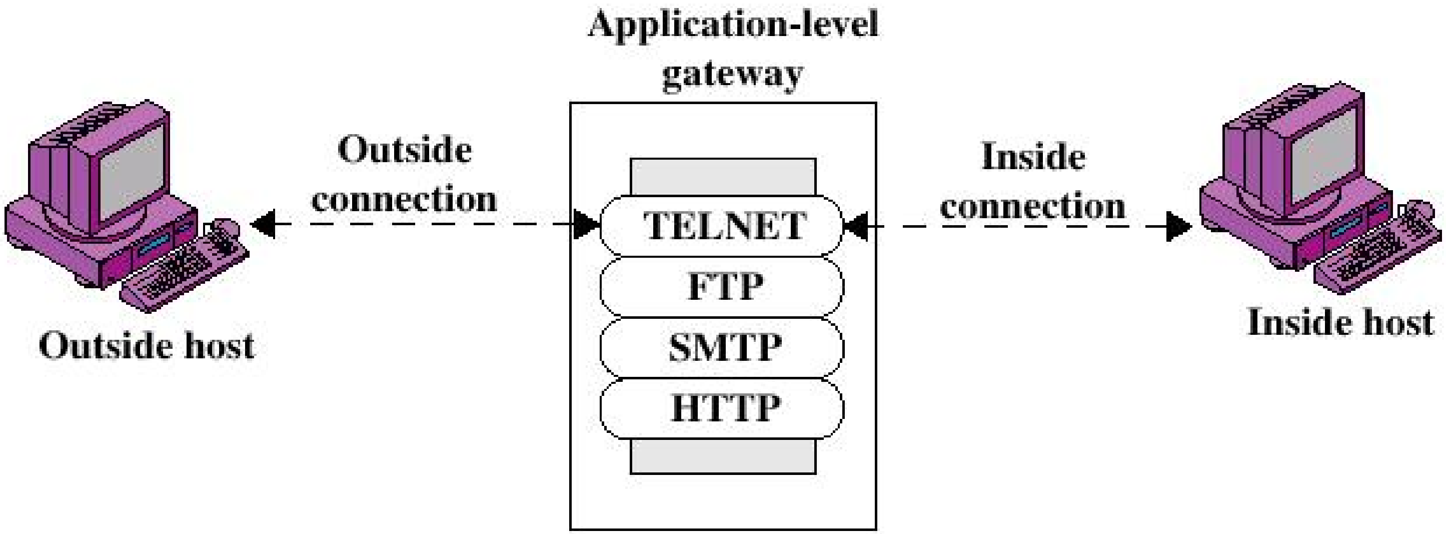
Stateful Inspection Firewalls

- Normal Packet Firewalls make decisions based on individual packets.
- In some cases higher layer context may be relevant.
- For example FTP
- 21 for control, 20 for data

Passive FTP



Application-level Gateway

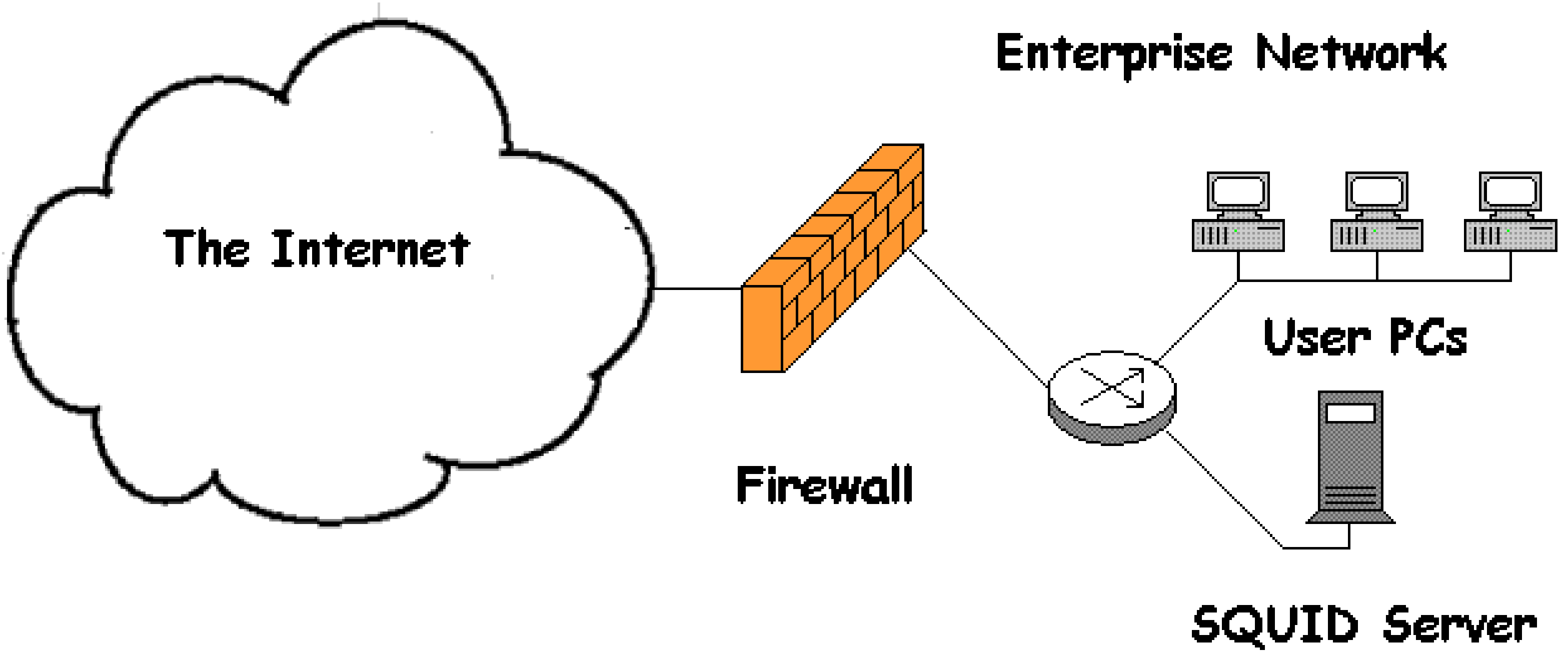


- Application-level Gateway
  - Also called application layer proxy server
  - Acts as a relay of application-level traffic

SQUID -an Application-level Gateway

- QUID–a very popular open source HTTP Proxy server.
- Widely used in LANS as a way of cutting down on traffic requesting web pages from external web servers.
- The following diagrams show how squid is used.

SQUID -an Application-level Gateway



One common Squid configuration involves sending user requests from PCs to the Squid server. The squid server checks to see if it has a cached copy of the requested web page. If it does it returns the page to the user's PC. If it doesn't, it requests the web page from the external web server on behalf of the client PC. When the page is returned, it keeps a copy in its web cache and also sends a copy of the page to the user. Future requests for the page by the user PCs will return the cached page. Web pages are cleared from the cache after a certain time.

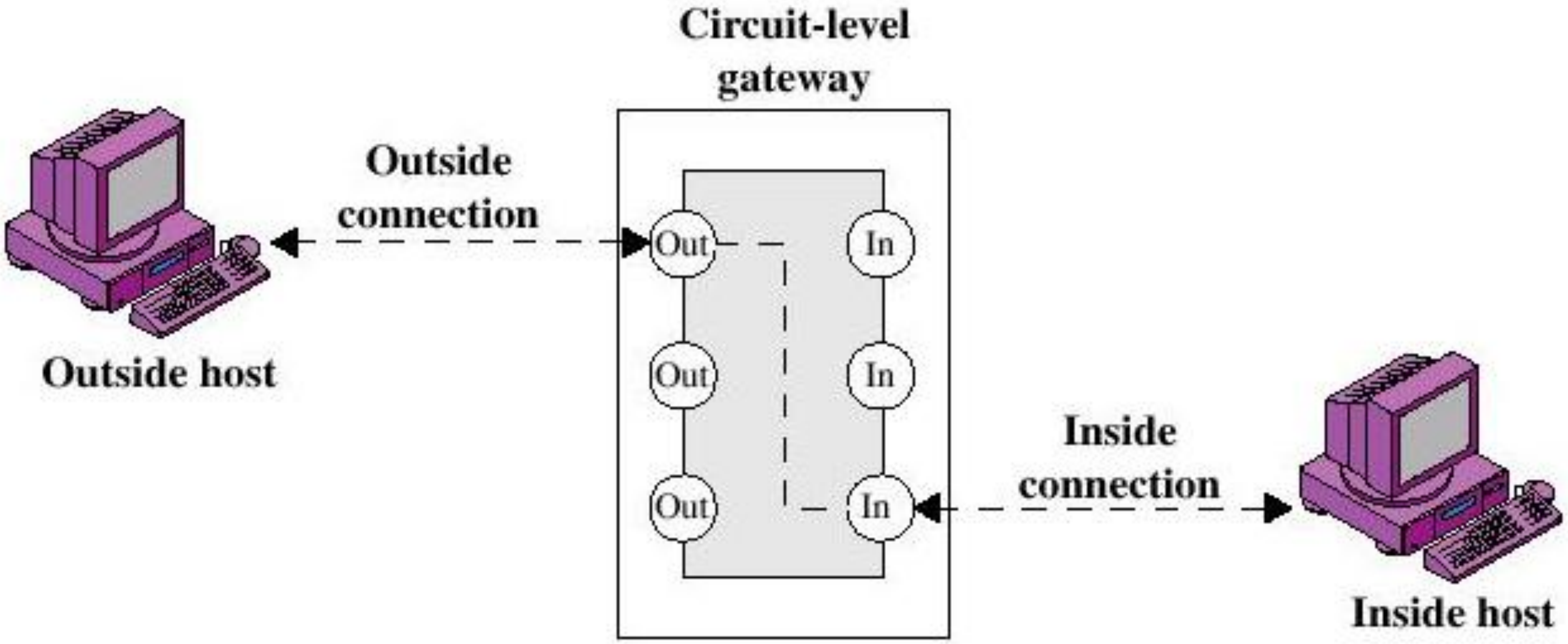
Application-level Gateway

- 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

Circuit-level Gateway

- Circuit-level Gateway



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

SOCKS –a proxy server

- SOCKS–A general purpose proxy server which works at the circuit level.
  - Current version is 5.
  - SOCKS V5 has been defined in RFCs 1928, 1929, 1961 and 3089.
  - Uses a special session level protocol to communicate with the proxied software.
  - Examines packets at the transport layer and makes decisions about whether particular client server connections are allowed.

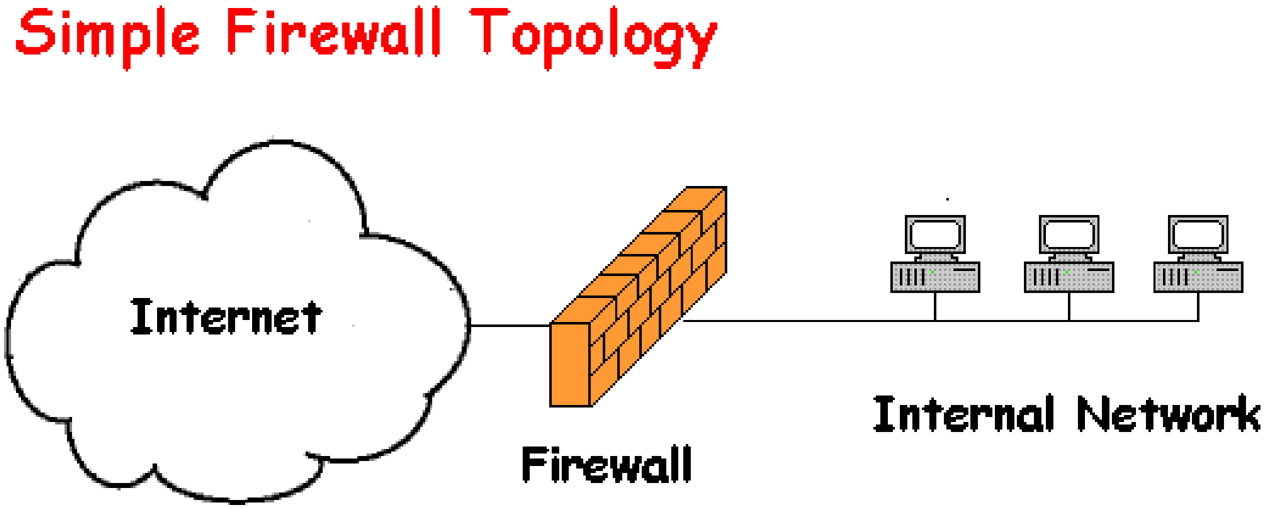
Circuit-level Gateway

- 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

Bastion Host

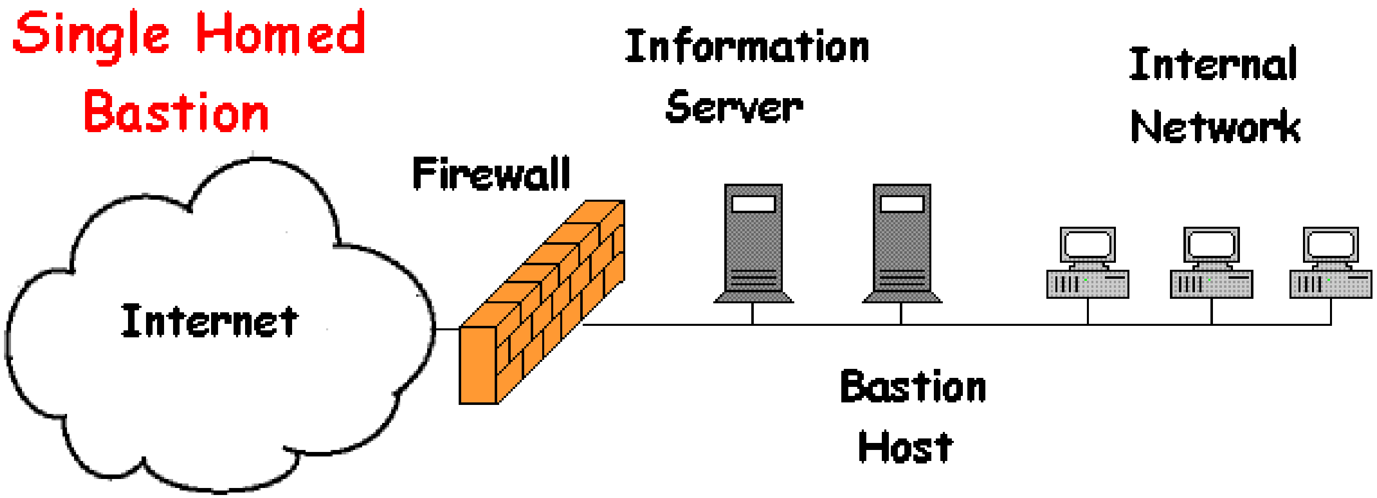
- A system identified by the firewall administrator as a critical strong point in the network's security
- The bastion host serves as a platform for an application-level or circuit-level gateway

Firewall Configurations Simple Topology



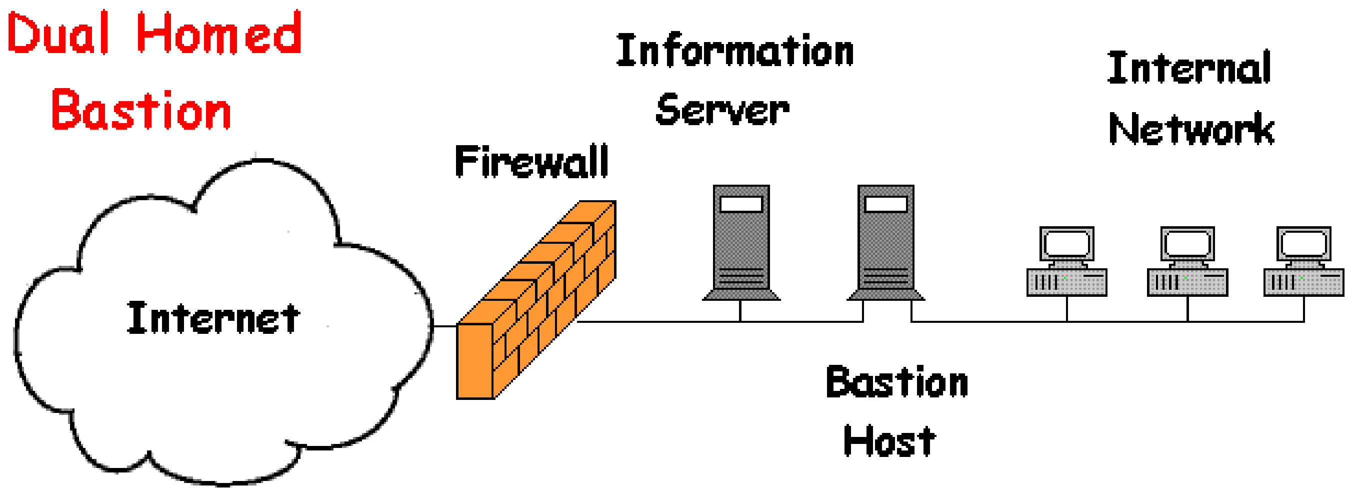
- This is the simplest firewall topology. In most cases the firewall is a packet filter firewall.

Single Homed Host



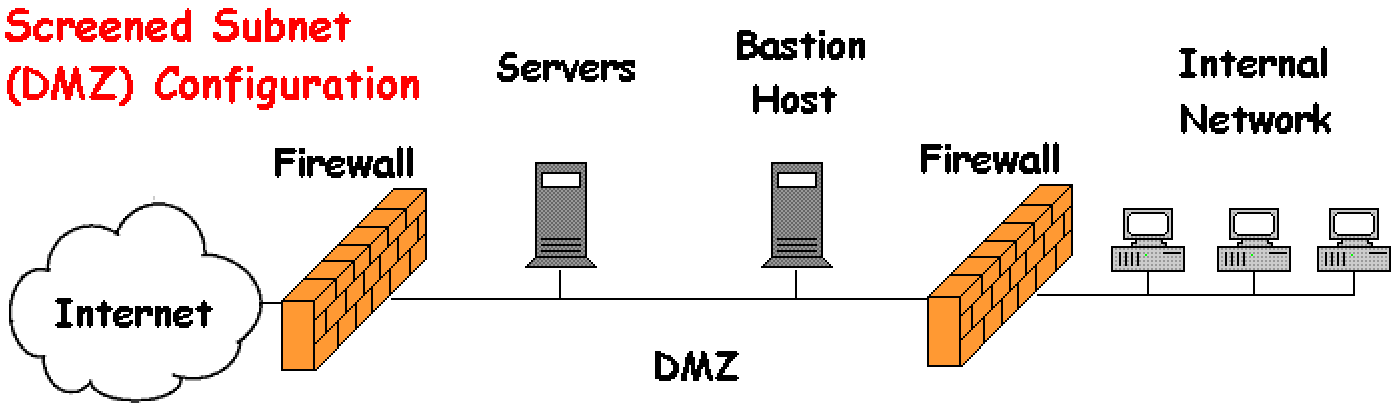
- A single-homed bastion host topology has a packet filter firewall with a bastion host (an application gateway) behind the firewall. The bastion host regulates access to the information server. It is also used to regulate access to the internet by the internal network PCs. The Information server may be allowed access to the internet through the packet filter firewall, but other devices on the internal network must access the internet through the bastion host.

Dual Homed Bastion



- A dual-homed bastion host topology has a packet filter firewall with a bastion host (an application gateway) behind the firewall. The bastion host regulates access to the information server. It is also used to regulate access to the internet by the internal network PCs as all access to the internet by the internal network hosts must go through the dual homed host. This system affords more security as even if the firewall is compromised, the internal network is still invisible.

DMZ



- A screened subnet topology has a packet filter firewall with a bastion host (an application gateway) behind the firewall. There is another packet filter firewall between the bastion host and the internal network. The space between the two packet filtering firewalls is known as a DMZ (demilitarised zone). The DMZ contains all the publicly available servers of the organisation. This is a very secure configuration.