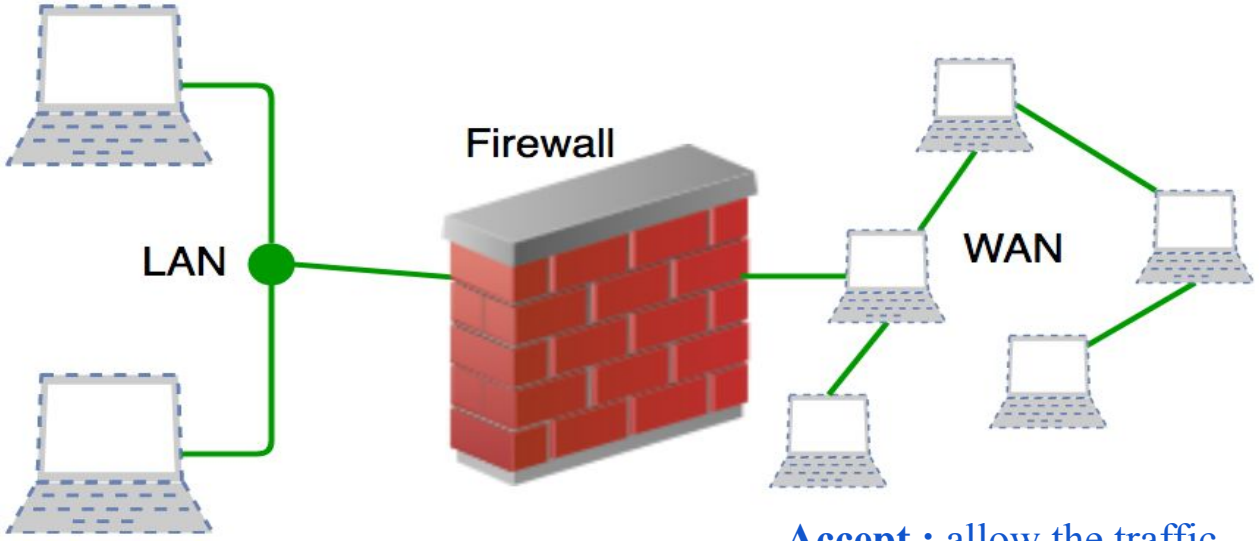
Firewalls

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.



Accept : allow the traffic

Reject : block the traffic but reply with an “unreachable error”

Drop : block the traffic with no reply

A firewall may be implemented in hardware as a stand-alone "firewall appliance" or in software on a PC.

➢ A single firewall may be adequate for small businesses and homes. However, in several large enterprises, multiple firewalls are deployed to achieve defence in depth.

Question: List and explain the functions of a firewall

Firewall Functionality:

Access Control:

✓ A firewall filters incoming (from the Internet into the organization) as well as outgoing (from within the organization to the outside) packets.

✓ A firewall is said to be configured with a rule set based on which it decides which packets are to be allowed and which are to be dropped.

Address/Port Translation:

✓ NAT was initially devised to alleviate the serious shortage of IP addresses by providing a set of private addresses that could be used by system administrators on their internal networks but that are globally invalid (on the Internet).

✓ it is possible to conceal the addressing schema of these machines from the outside world through the use of NAT.

✓ Through NAT, internal machines, though not visible on the Internet, can establish a connection with external machines on the Internet. NATing is often done by firewalls.

Logging. A sound security architecture will ensure that each incoming or outgoing packet encounters at least one firewall.

The firewall can log all anomalous packets or flows for later study.

✓ These logs are very useful for studying attempts at intrusion together with various worm and DDoS attacks.

Authentication: Some types of firewalls perform authentication of external machines attempting to establish a connection with an internal machine.

➢ A special type of firewall called web proxy authenticates internal users attempting to access an external service. Such a firewall is also used to cache frequently requested web pages. This results in decreased response time to the client while saving communication bandwidth.

Policies and Access Control Lists

➢ High-level policies for access to various types of services are formulated within an organization or campus. Examples of these include the following:

✓ All received e-mail should be filtered for spam and viruses.

All HTTP requests by external clients for access to authorized pages of the organization's website should be permitted.

✓ The organization's employees should be allowed to remotely log into authorized internal machines. However, all such communication should be authenticated and Encrypted.

Only two types of outgoing traffic are permitted.

First, all e-mail from within the organization to the outside world are permitted.

Second, requests eminating from within the organization for external web pages are permitted. However, requests for pages from certain "inappropriate" websites should be denied.

Question: Explain the different types of firewalls

Firewall Types: Firewalls can be classified into the categories

1. Packet Filters
2. Stateful Inspection
3. Application Level Firewalls

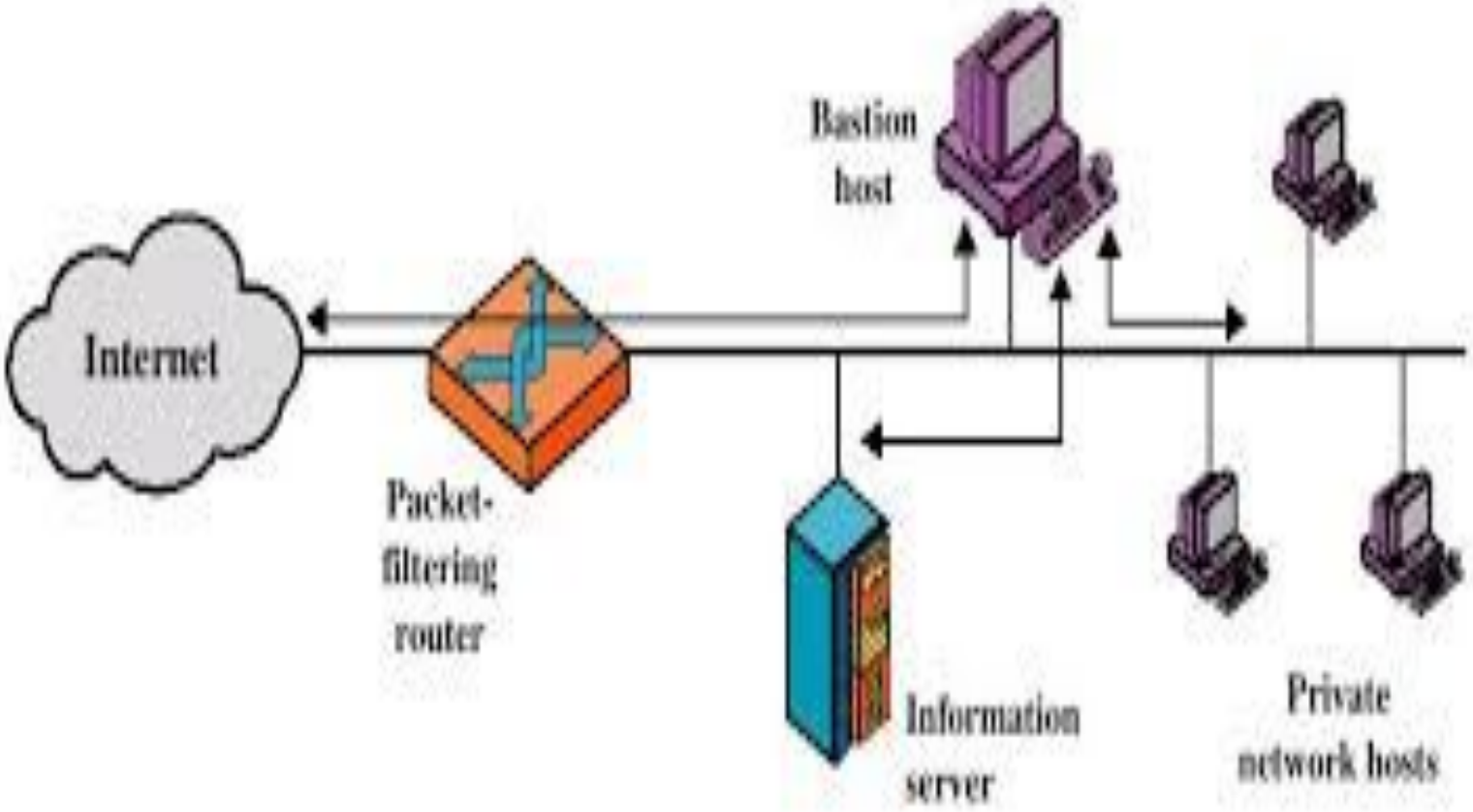
1. Packet Filters

➢ This involves checking for matches in the IP, TCP, or UDP headers.

➢ For example, it may be necessary to check whether a packet carries a certain specific source or destination IP address or port number.

➢ It is **often performed by the border router or access router** that connects the organization's network to the Internet.

➢ In effect, the border router becomes the first line of defence against malicious incoming packets.


Bastion host
Internet
Packet-filtering router
Information server
Private network hosts

Consider an external mail server (IP address = ABC) that wishes to deliver mail to an Organization. For this purpose, it should first establish a TCP connection with the organization's mail server, MS.

➢ Consider the arrival of a packet with the following attributes:

➢ Source IP address = ABC

➢ Destination IP address = MS

➢ TCP destination port = 25 (SMTP port)

➢ ACK flag set

➢ Such a packet would be part of a normal flow provided a connection between ABC to MS has been established. But suppose such a connection has not yet been established.Should the packet still be allowed in? The simple packet filter will allow the packet to enter even if no prior connection between ABC and MS was established.

➢ It should be noted that such packets are often used to perform port scans.

➢ A simple packet filter merely inspects the headers of an incoming packet in isolation. It does view a packet as part of a connection or flow. Hence, it will not be able to filter out such packets arriving from ABC.

Stateful Inspection

➢ A firewall uses packet TCP flags and sequence/acknowledgement numbers to determine whether it is part of an existing, authorized flow.

➢ If it is participating in the establishment of an authorized connection or if it is already part of an existing connection, the packet is permitted, otherwise it is dropped.

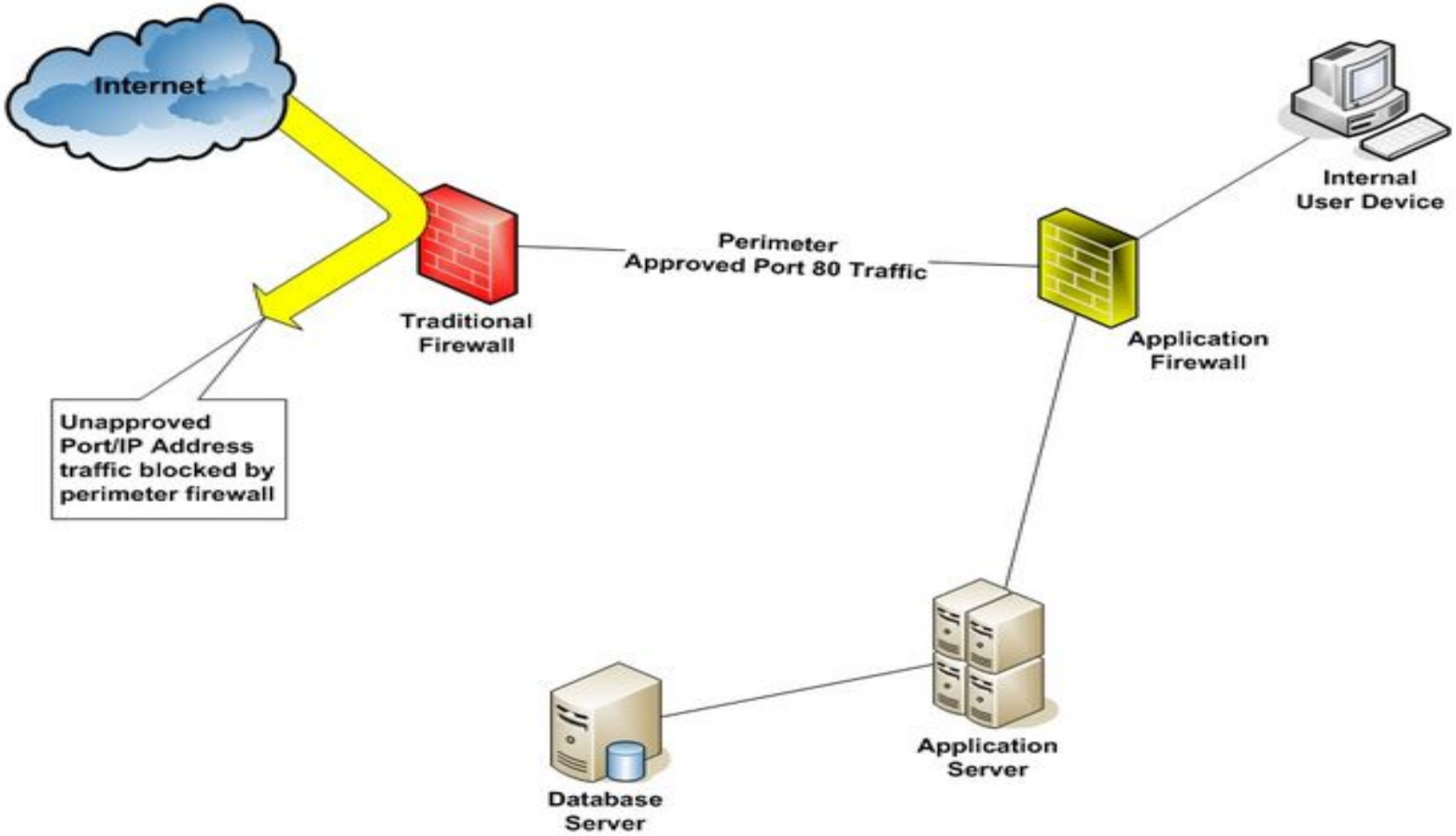
In the above example of the packet from ABC, the stateful packet inspection firewall will realize that it has not encountered the first two packets in the three-way handshake and will hence drop this packet.

Application Level Firewalls

➢ A packet-filtering firewall, even with the added functionality of stateful packet inspection, is still severely limited.

➢ What is needed is a firewall that can examine the application payload and scans packets for worms, viruses, spam mail, and inappropriate content. Such a device is called a deep inspection firewall.

➢ A special kind of application-level firewall is built using proxy agents. Such a "proxy firewall" acts as an intermediary between the client and server. The client establishes a TCP connection to the proxy and the proxy establishes another TCP connection with the server


Internet
Traditional Firewall
Perimeter
Approved Port 80 Traffic
Application Firewall
Internal User Device
Unapproved Port/IP Address traffic blocked by perimeter firewall
Database Server
Application Server

To a client, the proxy appears as the server and to the server, the proxy appears as the client. Since there is no direct connection between the client and the server, worms and other malware will not be able to pass between the two, assuming that the proxy can detect and filter out the malware. Hence, the presence of the proxy enhances security.

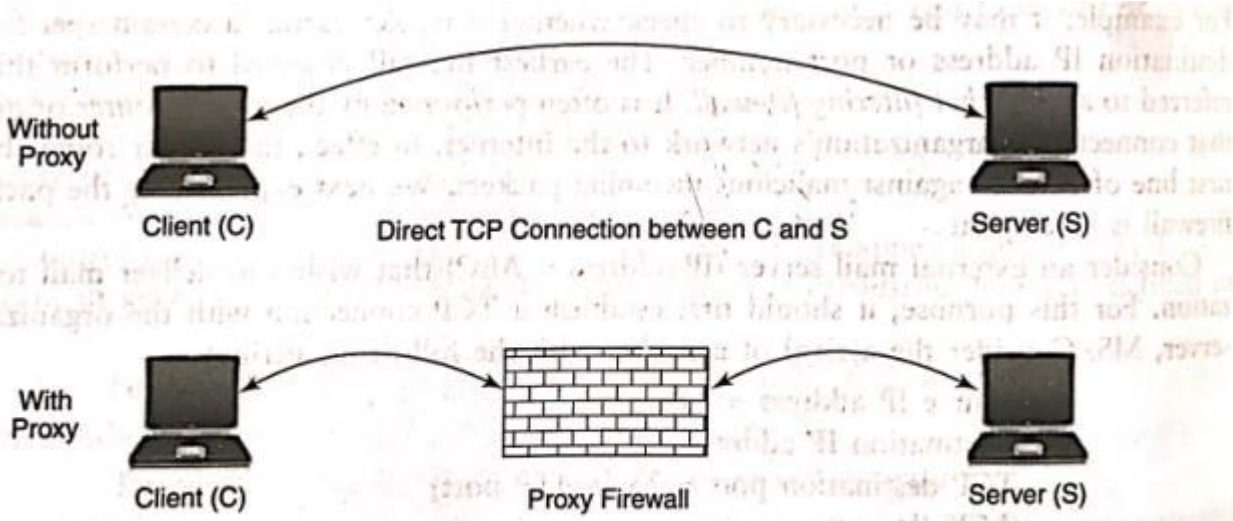


Figure 21.1 *Proxy firewall*

There are proxy agents for many application layer protocols including HTTP, SMTP, and FTP.

➢ In addition to filtering based on application layer data, proxies can perform client authentication and logging.

➢ An HTTP proxy can also cache web pages.

➢ Caching has a major impact on performance.

➢ If the webpage is cached in a web proxy server located in the client's organization, the response time could be greatly reduced compared to that where the page has to be fetched from the external web server.

➢ Also, caching reduces the demand on external communication bandwidth while easing the load on the web server.

➢ Firewalls are a necessary element in the security architecture of an organization that permit access to/from the external world.