Firewall

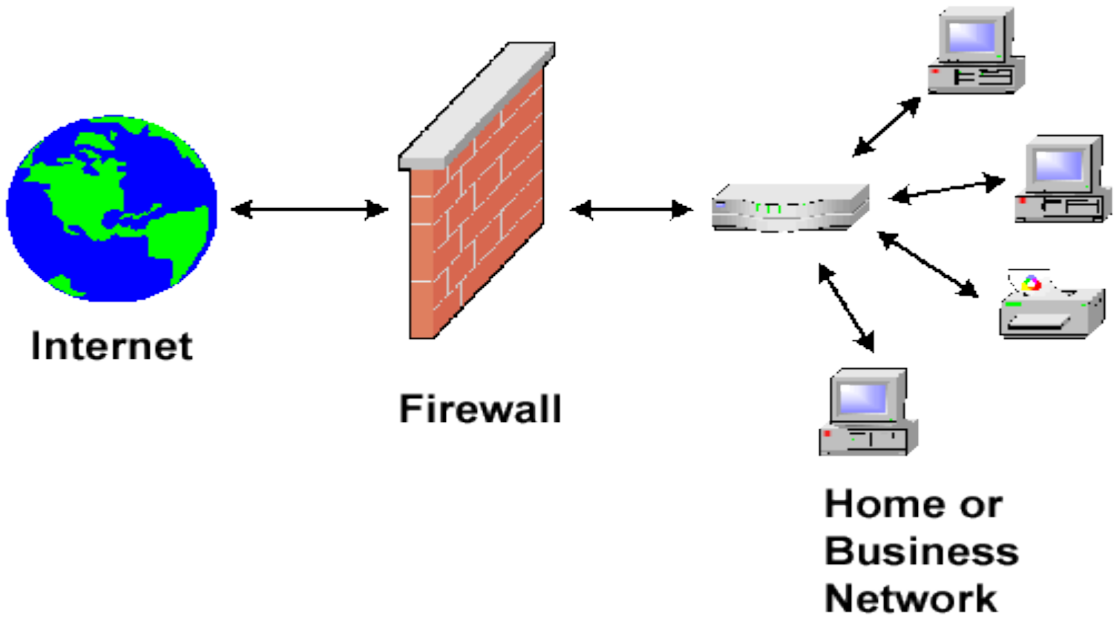
Prof Brijendra Singh
Department of Computer Science,
Lucknow University, Lucknow

A firewall is a device that filters all traffic between a protected or “inside” network and a less trustworthy or “outside” network.

Usually, a firewall runs on a dedicated device, because it is single point through which traffic is channeled, performance is important, which means non-firewall functions should not be done on the same machine.

Because a firewall is executable code, the attacker could compromise that code and execute from the firewall device.

The purpose of the fIrewall is to keep “bad” things outside a protected environment. To accomplish that, firewall implement a security that is specifically designed to address what bad thing’s might happen.



Packet-Filtering Firewalls

Packet-filtering firewalls or packet-filtering gateway applies a set of rules to each incoming IP packet and then forwards or discards the packets.

The router is typically configured to filter packets going in both directions (from and to the internal networK).

Stateful Inspection Firewalls

Filtering firewall work on packets one at a time, accepting or rejecting each packet and moving on to the next. They have no concept of “state” or “context” from one packet to the next. A stateful inspection firewall maintains state information from one packet to another in the input stream.

Proxy Firewalls

A proxy firewall also called an application layer firewalls, is a firewall that simulates the (proper) effects of an application, so that the application will receive only requests to act properly.

Guards

A guard is a sophisticated firewall. Like a proxy firewall, it receives protocol data units, interprets them, and passes through the same or different protocol data units that achieve either the same result or a modified results.

The guard decides what services to perform on the user's behalf in accordance with its available knowledge.

Personal Firewalls

A personal firewall is an application program that runs on a workstation to block unwanted traffic, usually from the network.

The personal firewall is configured to enforce some policy. For example, the user may decide that certain sites, such as computers on the company networks, are highly trustworthy but most other sites are not.

Limitations of Firewalls

1. The firewall cannot protect against attack that bypass the firewall.
2. The firewall does not protect against internal threats.
3. The firewall can not protect against the transfer of virus-infected programs or files.
4. The firewall can be “fooled” by source routing or address spoofing.

REFERENCE:

Book: Network Security and Management

Author: Prof Brijendra Singh

Publisher: PHI Learning Private Limited, New Delhi,