



Firewalls

Introduction

A firewall is a dedicated hardware or software device running on a computer, which inspects network traffic passing through it, and allows passage based on a set of rules.

Overview

Most firewalls are placed on the perimeter between the external network (usually the Internet) and the network to be protected.

Firewall types

Firewalls may be dedicated, host-based or embedded.

- A Dedicated Firewall is a computer solely used for firewall activities, its purpose is to separate networks.
- A Host-based Firewall is a service that runs on a user terminal or workstation.
- An Embedded Firewall is a border device such as a router that has built in firewall capabilities and is used to protect the local network. It is a useful line of defence but it is not recommended as a primary firewall.

Firewall position on a network

Firewalls may be set at the exterior or the interior of a network

- 'Exterior' firewalls are placed on the perimeter between the external network and the internal network.
- 'Internal' firewalls are placed on the internal network to separate internal network segments.

Benefits and limitations of a Firewall

Benefits

Firewalls allow administrators to offer access to specific types of Internet services. Privileges can be granted according to the job description.

Limitations

Firewalls can constitute a traffic bottleneck. They concentrate security in one spot and then create a single point of failure.

