# Security Functions of Firewalls

Firewalls are security devices designed to control traffic and protect networks from each other they're usually applied to protect high trust networks from low trust ones or to stop networks part of the same organization but from different departments. They can be either hardware or software.

There are four different types of firewalls:

**Packet filter Firewalls** – uses the packet header to do basic traffic filtering usually based of the source and destination address, port numbers and protocols. They operate in the network and transport layers of the OSI model.

**Circuit-level Gateways** – filters traffic between internal trusted host and external untrusted host. It operates at the network and session layer of the OSI. This type of firewall ensures that the packets used to make the connection are used in the proper way. Once a connection is established no further filtering occurs.

**Application level firewalls** – filters traffic at the application layer of the OSI model, it bases its filtering on the user access, group membership, applications and services or even the type of resources being transmitted. This type of firewalls focuses on the characteristic of specific appliances and protocol combination and the type of content of the communication.

**State full inspection firewalls** – state full packet inspection (SPI) means that the firewall remembers the state of the connection or session (TCP/UDP), it automatically creates a rule for the reply packet based on the type of communication

used. This rule stays as long as the connection remains; when the connection terminates the rule is deleted.

The first step taken when deploying firewalls is to create a firewall security policy, this policy states the scope of the firewall, the networks it needs to protect, the type of services, applications, devises, users that are allowed or disallowed.

Many firewalls have two or more NICs and thus they're called dual-homed or multi-homed firewalls. The distinction of these firewalls is that for traffic to pass from one network to the other they most satisfy the rules on this firewall. Therefore in this way firewalls are able to provide a reliable and strong security.

Firewalls that have more than two NICs are able to dedicate one of these NICs to host DMZ devices; DMZs are zones containing devices that should be publicly available such as DNSs, Web, FTP servers, etc. It provides public but secure access to DMZ devices and prevents unauthorised access to private network. If this firewall is compromised then only the DMZ devices are at risk, while the private network remains secure to some extent unless the attacker manages to exploit the trust relationship of the devices to penetrate through the network.

Firewalls are unable to read or inspect encrypted data, thus if the port to enable VPN connections is open traffic dedicated to this port will go through the firewall without being inspected, which in a security point of view could provide a vulnerability.

Source : http://infosectutorials.com/2012/03/04/1-network-security-part-1/