

Security and Firewall

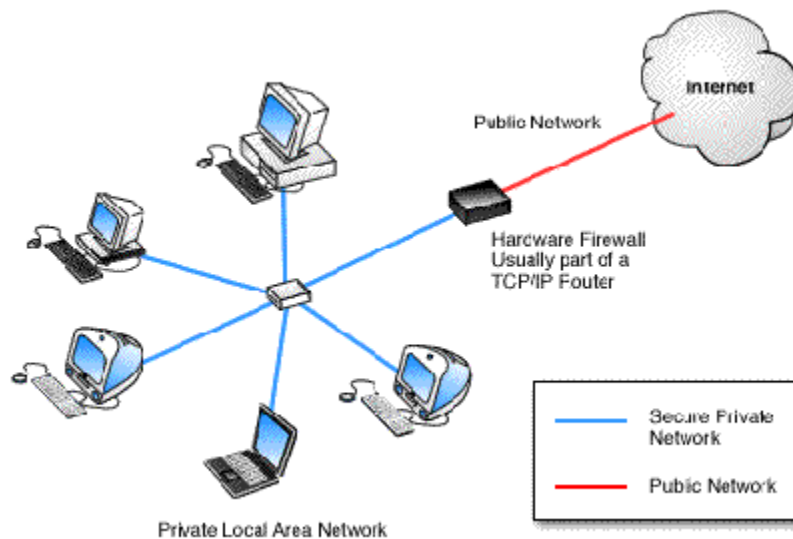
July 2000

Firewalls

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. A Firewall in its most simplistic sense, controls the flow of traffic. It may be a hardware device or a software program running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet. The earliest firewalls were simply routers.

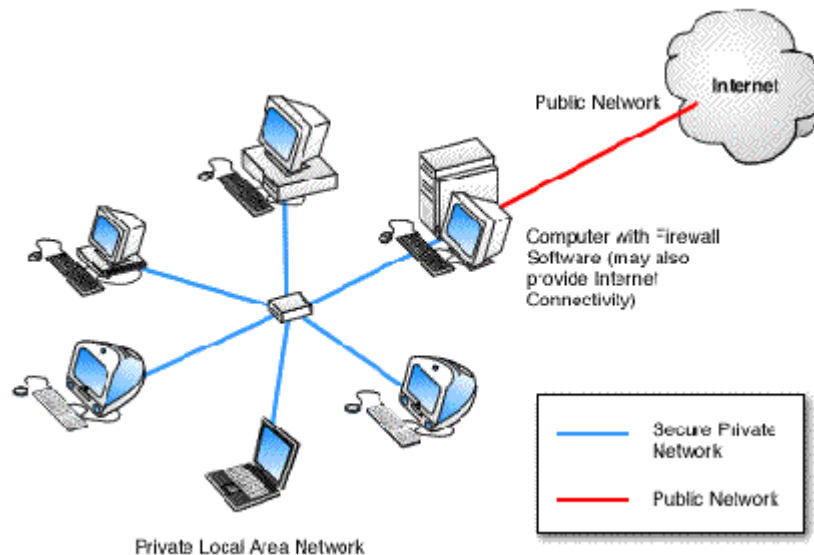
Hardware Firewall

Hardware firewall providing protection to a Local Network



Computer with Firewall Software

Computer running firewall software to provide protection



Functions of Firewalls

A firewall examines all traffic routed between the two networks to see if it meets certain criteria, if it does, it is routed between the networks, otherwise it is stopped. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state.

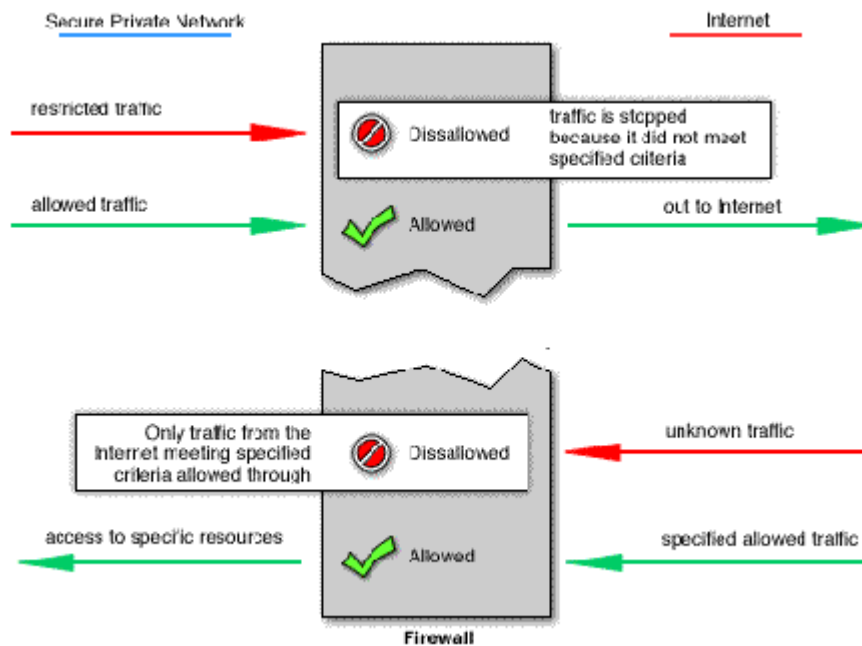
Who needs a firewall?

Anyone who is responsible for a private network that is connected to a public network needs firewall protection. Furthermore, anyone who connects so much as a single computer to the Internet via modem should have personal firewall software.

How does a firewall work?

There are two access denial methodologies used by firewalls. A firewall may allow all traffic through unless it meets certain criteria, or it may deny all traffic unless it meets certain criteria. The type of criteria used to determine whether traffic should be allowed through varies from one type of firewall to another. Firewalls may be concerned with the type of traffic, or with source or destination addresses and ports. They may also use complex rule bases that analyze the application data to determine if the traffic should be allowed through. How a firewall determines what traffic to let through depends on which network layer it operates at. A discussion on network layers and architecture follows.

Basic Firewall Operation



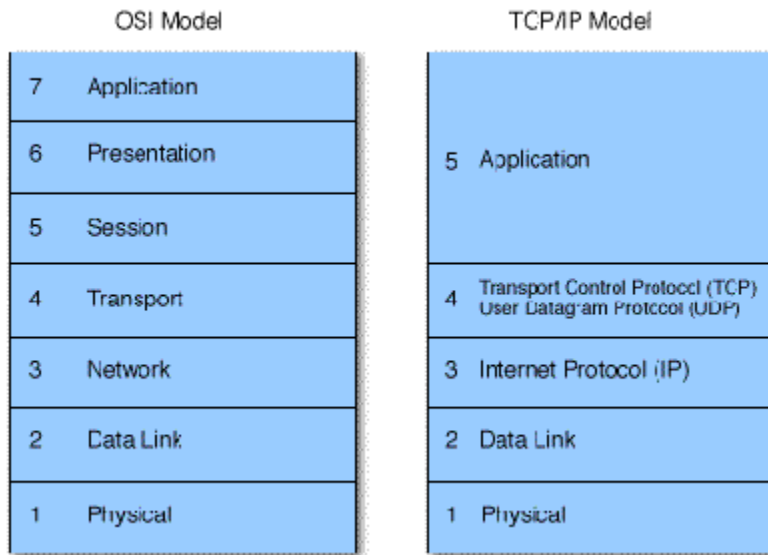
What are the OSI and TCP/IP Network models?

To understand how firewalls work it helps to understand how the different layers of a network interact. Network architecture is designed around a seven-layer model. Each layer has its own set of responsibilities, and handles them in a well-defined manner. Firewalls operate at different layers to use different criteria to restrict traffic.

The lowest layer at which a firewall can work is layer three. In the OSI model this is the network layer. In TCP/IP it is the Internet Protocol layer. This layer is concerned with routing packets to their destination. At this layer a firewall can determine whether a packet is from a trusted source, but cannot be concerned with what it contains or what other packets it is associated with.

Firewalls that operate at the transport layer know a little more about a packet, and are able to grant or deny access depending on more sophisticated criteria. At the application level, firewalls know a great deal about what is going on and can be very selective in granting access.

The OSI and TCP/IP models



It would appear then, that firewalls functioning at a higher level in the stack must be superior in every respect. This is not necessarily the case. The lower in the stack the packet is intercepted, the more secure the firewall. If the intruder cannot get past level three, it is impossible to gain control of the operating system.

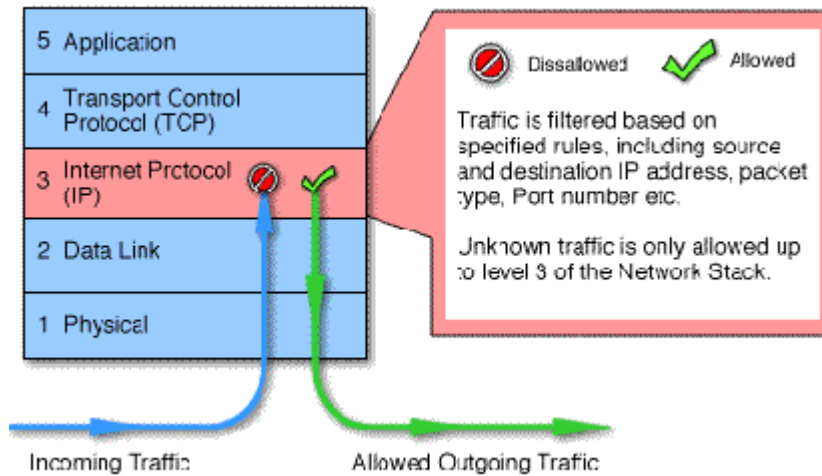
What different types of firewalls are there?

Firewalls fall into four broad categories: packet filters, circuit level gateways, application level gateways and stateful multilayer inspection firewalls.

Packet Filtering Firewall

Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP. They are usually part of a router. These firewalls rely solely on TCP, UDP, ICMP, and IP headers of individual packets to permit or deny traffic. The packet filter looks at a combination of traffic direction (inbound or outbound), IP source and destination address, and TCP or UDP source and destination port numbers.

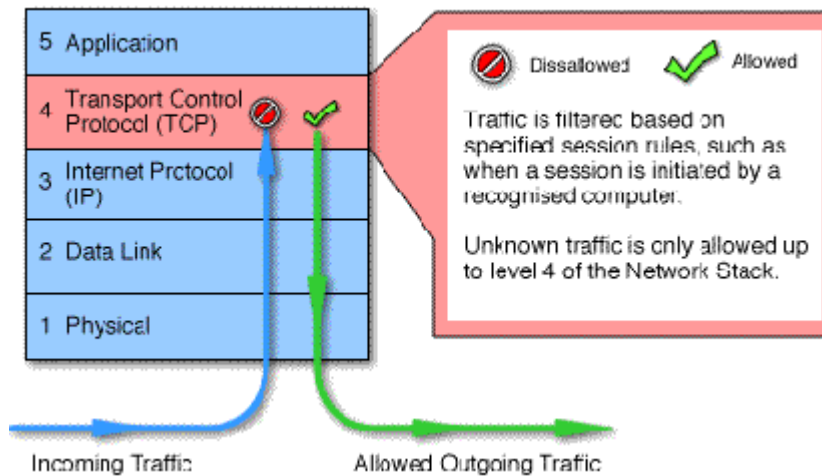
Packet Filtering Firewall



Circuit Filtering

Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. These firewalls control access by keeping state information and reconstructing the flow of data associated with the traffic. A circuit filter won't pass a packet from one side to the other unless it is part of an established connection.

Circuit level Gateway

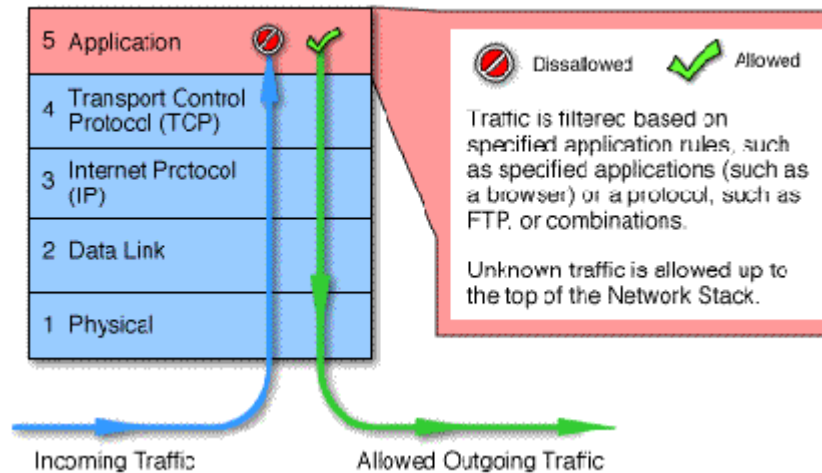


Application Gateway

Application level gateways, also called proxies, are similar to circuit-level gateways except that they are application specific. They can filter packets at the application layer of the OSI model. Incoming or outgoing packets cannot access services for which there is no proxy. In plain terms, an application level gateway that is

configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through. Application level gateways can also be used to log user activity and logins. They offer a high level of security, but have a significant impact on network performance. This is because of context switches that slow down network access dramatically. They are not transparent to end-users and require manual configuration of each client computer.

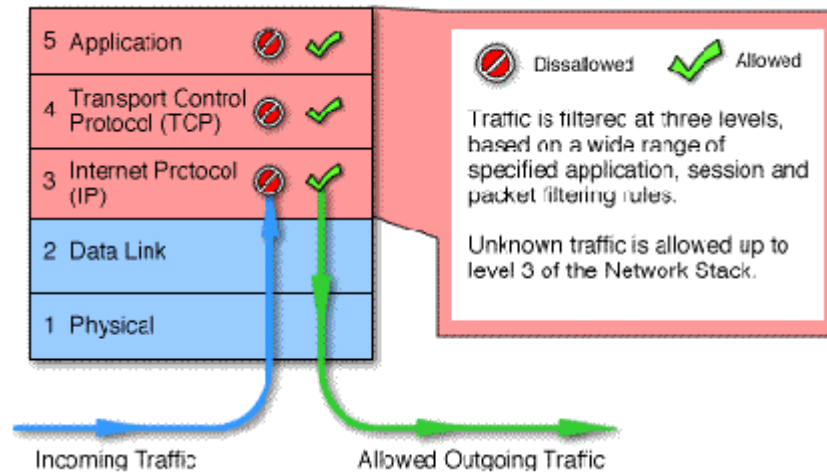
Application level Gateway



Stateful Inspection

Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls. They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer. They allow direct connection between client and host, alleviating the problem caused by the lack of transparency of application level gateways. They rely on algorithms to recognize and process application layer data instead of running application specific proxies. Stateful multilayer inspection firewalls offer a high level of security, good performance and transparency to end-users. They are expensive however, and due to their complexity are potentially less secure than simpler types of firewalls if not administered by highly competent personnel.

Stateful Multilayer Inspection Firewall



Is a firewall sufficient to secure network or needed anything else?

The firewall is an integral part of any security program, but it is not a security program in and of itself. Firewalls only address the issues of data integrity, confidentiality and authentication of data that is behind the firewall. Any data that transits outside the firewall is subject to factors out of the control of the firewall. It is therefore necessary for an organization to have a well planned and strictly implemented security program that includes but is not limited to firewall protection.