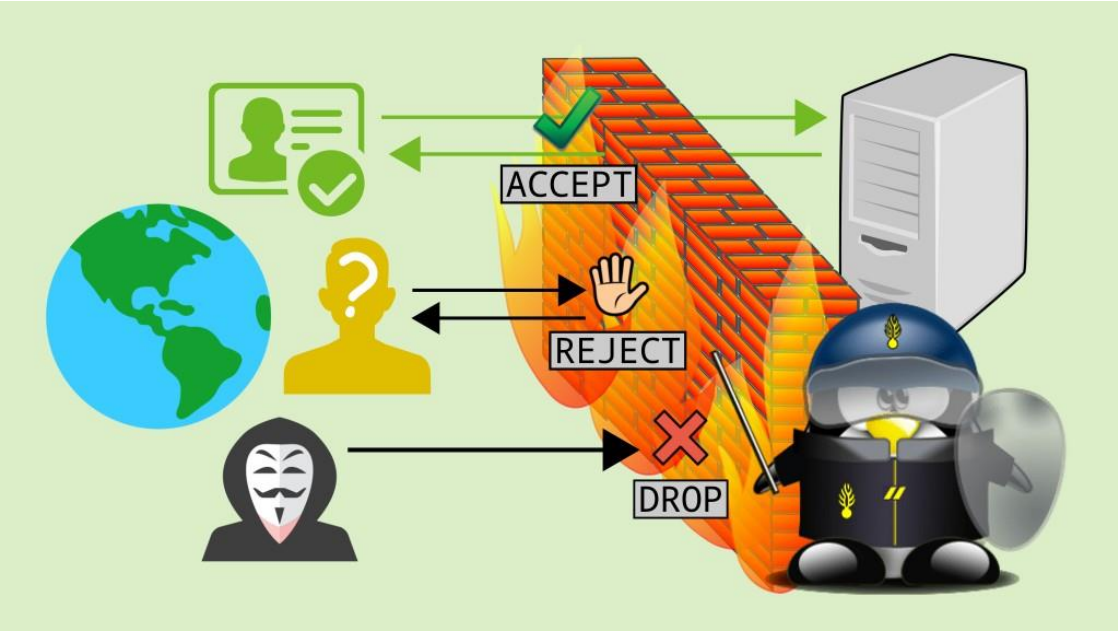
Firewalls

Introduction

- A Firewall manages the secure in-flow and out-flow of data in a device. It monitors the network traffic and acts as a barrier between the trusted and untrusted network.
- A Firewall is a security system to protect an internal network from unauthorized servers and networks based on predefined rules. It acts as a barrier and only allows the secured network to send or receive data.

How does a Firewall work?

- Firewall analyses the network traffic and filters it so that the unsecured and suspicious networks cannot attack the system.
- The point where information is exchanged with an external network is called a port.



History and Development of Firewall

- The term 'Firewall' actually meant a wall which intended to confine a fire within a line of adjacent buildings. It was only in the late 1980s when this was acknowledged as a computer terminology.
- It was during this time that the Internet has started to emerge as a new tool for global use. Thus, having a means which could secure the transmission and flow of data was required by many.
- Until the Firewall was introduced, routers performed the same function as it restricted the number of people who could use a particular network.

Firewall Environments

- There are different types of environments where a firewall can be implemented.
- Simple environment can be a packet filter firewall
- Complex environments can be several firewalls and proxies

Functions of Firewall

- Any data which enters or exits a computer network has to pass through the Firewall
- All the valuable information stays intact if the data packets are securely passed through the Firewall
- Every time a data packets passed through a Firewall, it records it which allows the user to record the network activity
- No data can be modified as it is held securely within the data packets

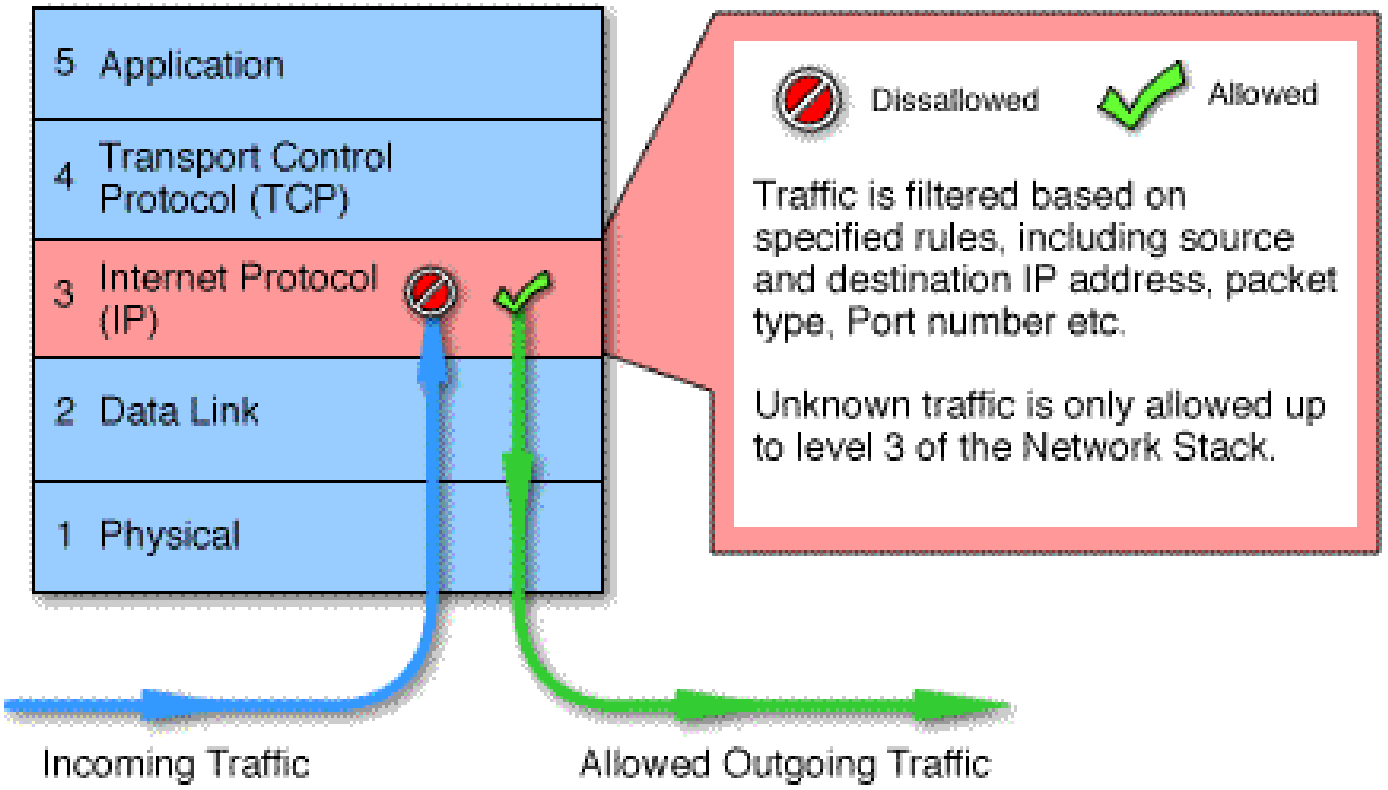
Types of Firewall

- Packet filters
- Circuit level
- Application level
- Stateful multilayer
- Next-Generation Firewall
- Software Firewall
- Hardware Firewall

Packet Filter

- Work at the network level of the OSI model
- Each packet is compared to a set of criteria before it is forwarded
- Packet filtering firewalls is low cost and low impact on network performance

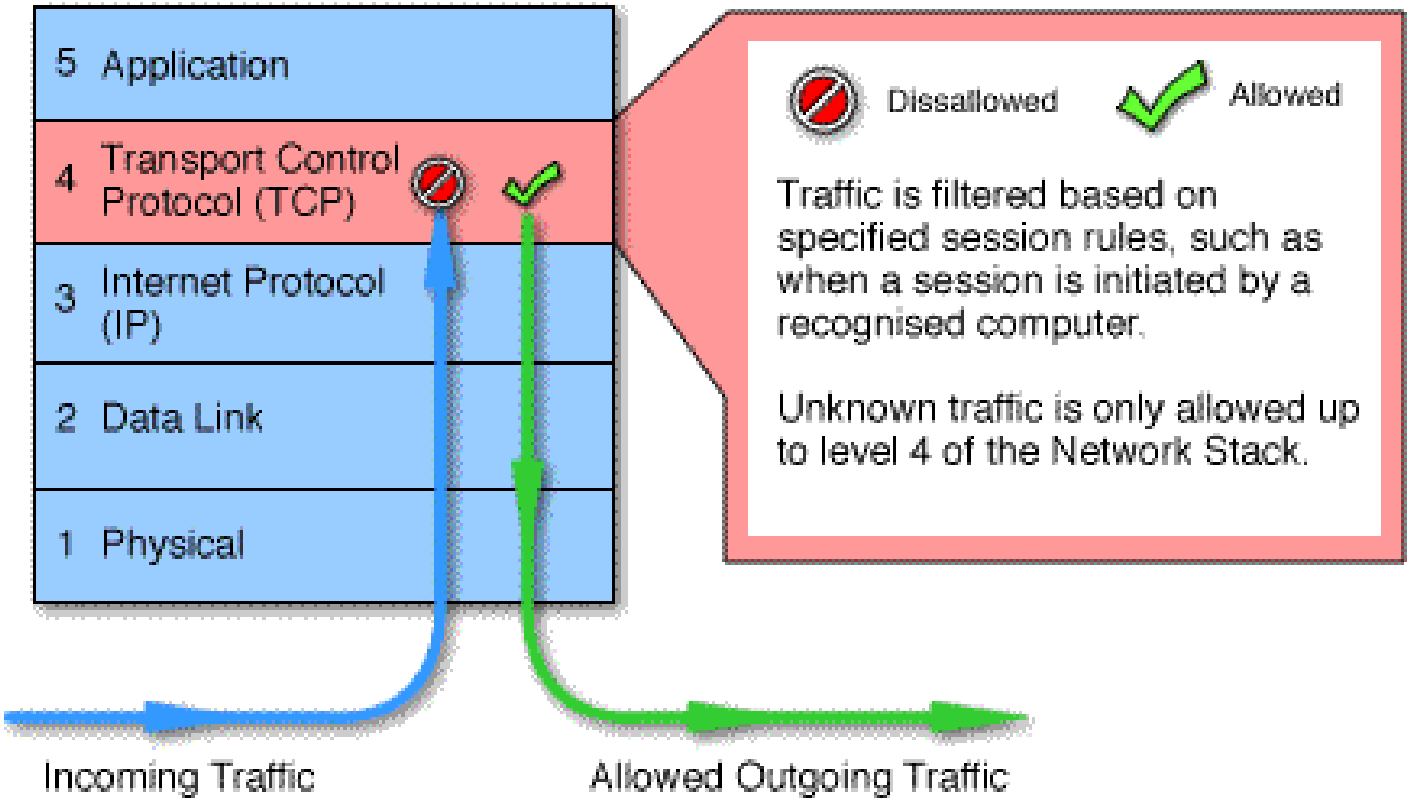
Packet Filtering



Circuit level

- Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP
- Monitor TCP handshaking between packets to determine whether a requested session is legitimate.

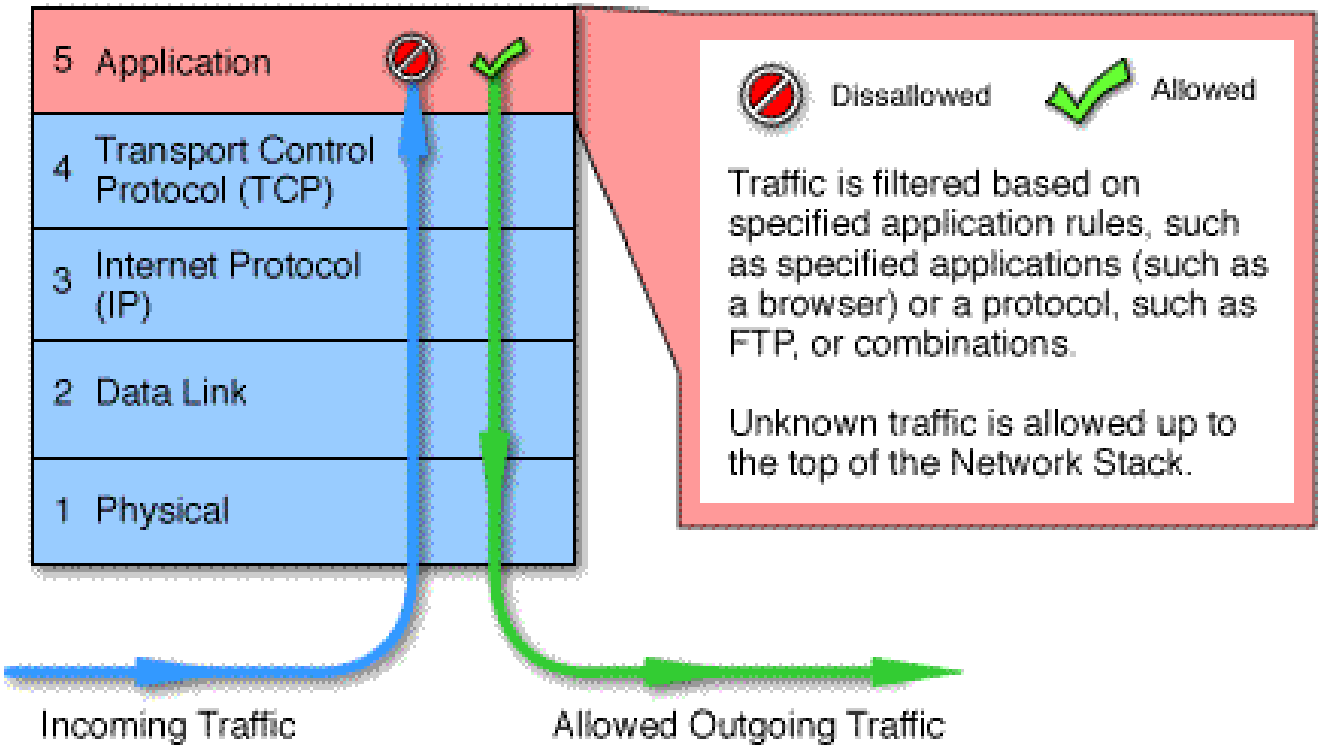
Circuit level



Application Level

- Application level gateways, also called proxies, are similar to circuit-level gateways except that they are application specific
- Gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through

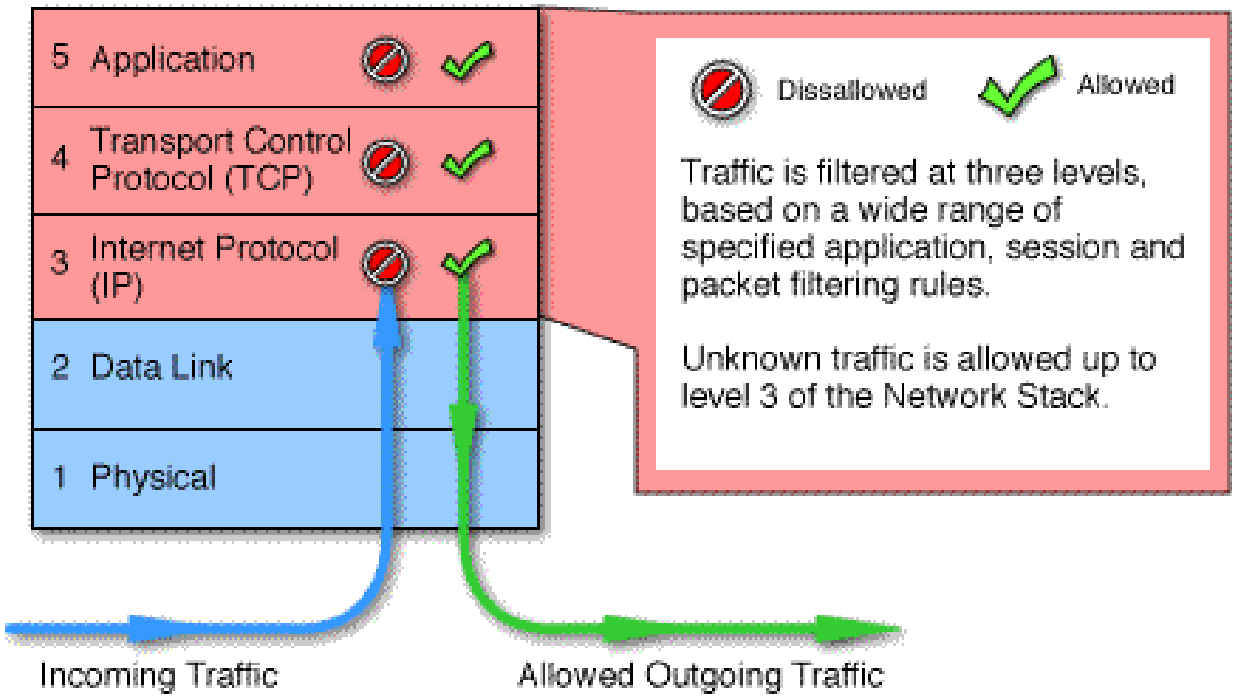
Application Level



Stateful Multilayer

- 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

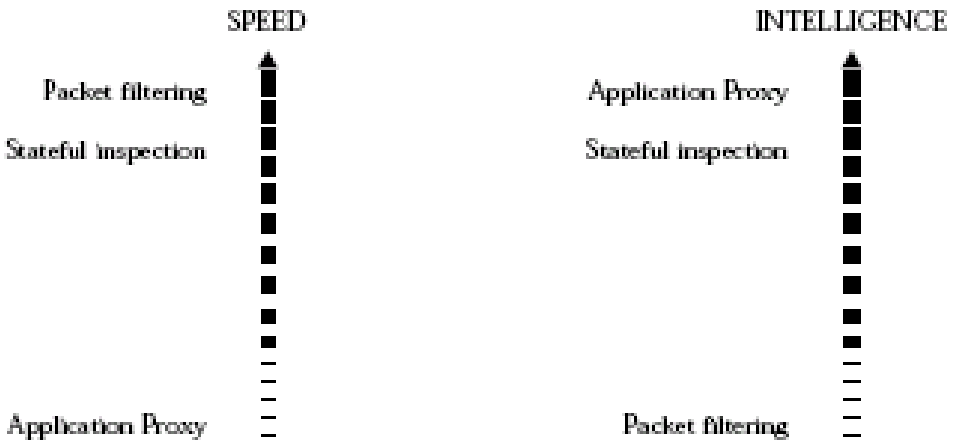
Stateful Multilayer



General Performance

FIREWALL PERFORMANCE SUMMARY

Technology	Speed	Flexibility	Intelligence
Packet filtering	V. Good	V.Good	Low
Application Proxy	Low	Low	V. Good
Stateful inspection	Good	Good	Good
Circuit gateway	Low	Low	Low



Next-Generation Firewall

- The recently launched Firewall systems are known as the Next-Gen Firewalls
- Under this, the data packets are also thoroughly checked before being passed on to the destination address
- These are still on the platform of improving and evolving and intend to use modern technology for automatic detection of errors and network safety

Software Firewall

- Any firewall which is installed in a local device or a cloud server is called a Software Firewall
- They can be the most beneficial in terms of restricting the number of networks being connected to a single device and control the in-flow and out-flow of data packets
- Software Firewall also time-consuming

Hardware Firewall

- They are also known as Physical-appliance based firewalls
- It ensures that the malicious data is stopped before it reaches the endpoint of the network at risk

Future of Firewalls

- Firewalls will continue to advance as the attacks on IT infrastructure become more and more sophisticated
- More and more client and server applications are coming with native support for proxied environments
- Firewalls that scan for viruses as they enter the network and several firms are currently exploring this idea, but it is not yet in wide use

Conclusion

- It is clear that some form of security for private networks connected to the Internet is essential
- A firewall is an important and necessary part of that security, but cannot be expected to perform all the required security functions.