Firewall Technologies

Presented by:
Fahad Shahzad
Muntazir Mehdi

Outlines

- Introduction
- Firewall
- Type of Firewalls
- Architecture of firewall technologies
- Conclusion

About firewall

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Intranet and Extranet

Characteristics

- Firewalls control the flow of network traffic
- Firewalls have applicability in networks where there is no internet connectivity
- Firewalls operate on number of layers
- Can also act as VPN gateways
- Active content filtering technologies

Firewall Architecture

- Dual-Homed Host Architecture
- Screened Host Architecture
- Screened Subnet Architecture
- Screening router

Dual home host architecture

Firewall dual-homing provides the first-line defense and protection technology for keeping untrusted bodies from compromising information security by violating trusted network space.

Screened host architecture

This architecture combines the packet filtering router with a separate, dedicated firewall, such as an application proxy server. This approach allows the router to pre-screen packets to minimize the network traffic and loads on the internal proxy.

Cont...

The application proxy examines an application layer protocol, such as HTTP, and perform the proxy services. This separate host is often referred to as a bastion host; it can be a rich target for external attacks, and should be very thoroughly secured.

Screened subnet architecture

In network security, a screened subnet firewall is a variation of the dual-homed gateway and screened host firewall. It can be used to separate components of the firewall onto separate systems, thereby achieving greater throughput and flexibility, although at some cost to simplicity. As each component system of the screened subnet firewall needs to implement only a specific task, each system is less complex to configure.

Screening router

A screening router performs packet-filtering and is used as a firewall. In some cases a screening router may be used as perimeter protection for the internal network or as the entire firewall solution.

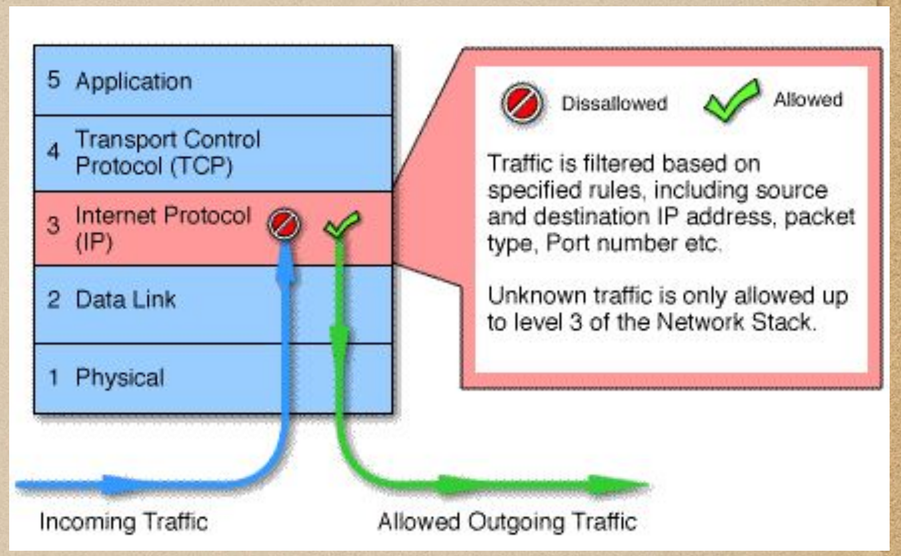
Types of firewall

Firewalls fall into six broad categories

- Packet filters
- Circuit level
- Application level
- Stateful multilayer
- Transparent Firewall
- Next Generation Firewall

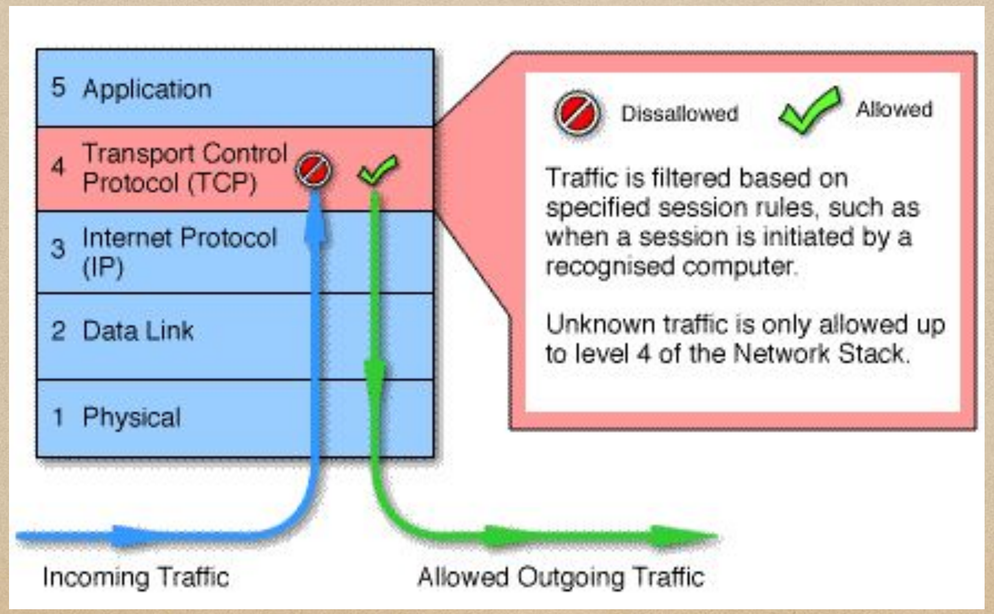
Packet Filter

- 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



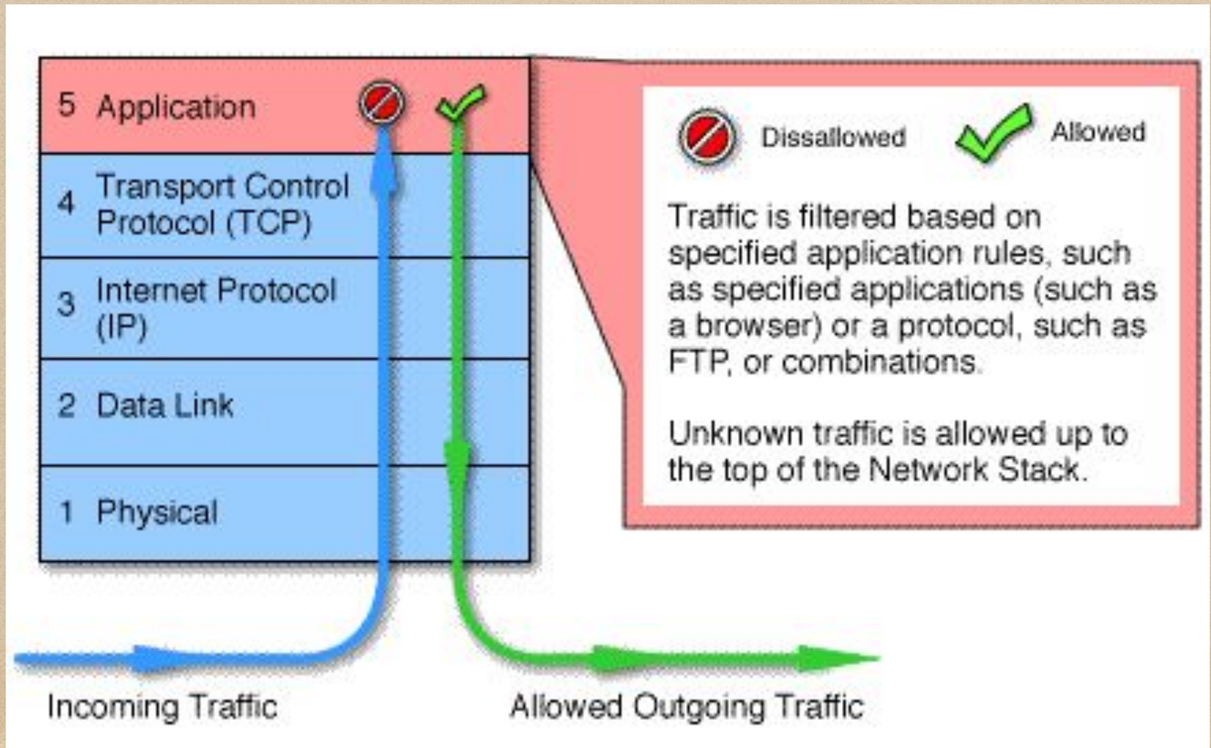
Circuit level

- 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.



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



Transparent firewall

Transparent firewalls are devices that you place within a single subnet to control traffic flow across a bridge. They allow you to insert a firewall on a subnet without renumbering your networks.

Next Generation Firewall

A next-generation firewall is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functions, such as an application firewall using in-line deep packet inspection, an intrusion prevention system

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.