A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. There are different types of firewalls available to protect your network from unwanted traffic.

PACKET-FILTERING FIREWALL:

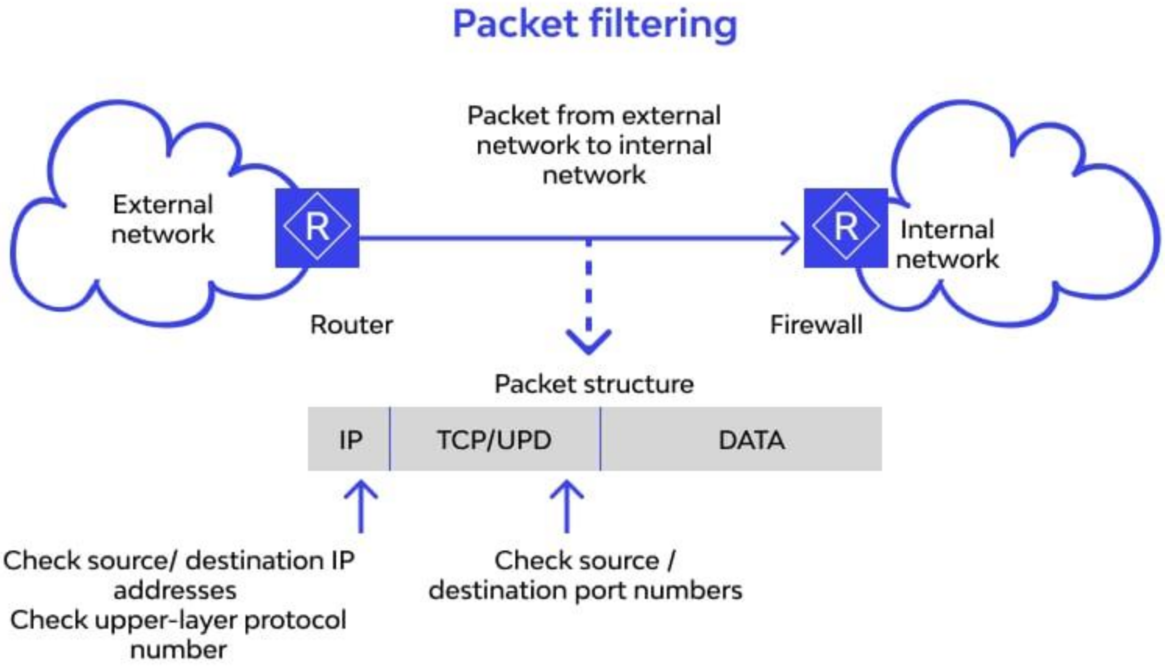
Packet-filtering firewalls operate at the network layer (Layer 3) of the OSI model. They examine individual packets of data based on predetermined rules and criteria, such as source/destination IP addresses, ports, and protocols.

STRENGTHS:

- Simplicity: Packet-filtering firewalls are straightforward to configure and operate, making them suitable for high-speed environments.
- Efficiency: They are typically fast and have minimal impact on network performance.
- Basic protection: Packet-filtering firewalls can block specific ports or IP addresses, providing a basic level of security against unauthorized access.

WEAKNESSES:

- Lack of visibility: Packet-filtering firewalls do not inspect the content of packets beyond basic header information, which limits their ability to detect more sophisticated attacks.
- Vulnerable to IP spoofing: Since they rely on IP addresses for filtering packet filtering firewalls can be tricked by attackers who forge their IP addresses.
- Limited protocol awareness: They do not have advanced knowledge of specific protocols, which makes them less effective in detecting application-layer attacks


Packet filtering
Packet from external network to internal network
External network
R
R
Internal network
Router
Firewall
Packet structure
IP
TCP/UPD
DATA
Check source/ destination IP addresses
Check upper-layer protocol number
Check source / destination port numbers

STATEFUL FIREWALL:

Stateful firewalls, also known as dynamic packet-filtering Firewalls, operate at the transport layer

(Layer 4) of the OSI model. In addition to examining packet headers, they track the state of network connections to make more informed filtering decisions

STRENGTHS:

- Connection tracking: Stateful firewalls maintain information about active connections, enabling them to differentiate between legitimate packets belonging to established connections and suspicious ones.

Improved security: By understanding the context of network traffic, stateful firewalls can enforce more granular access control policies and detect certain types of attacks that packet filtering firewalls might miss.

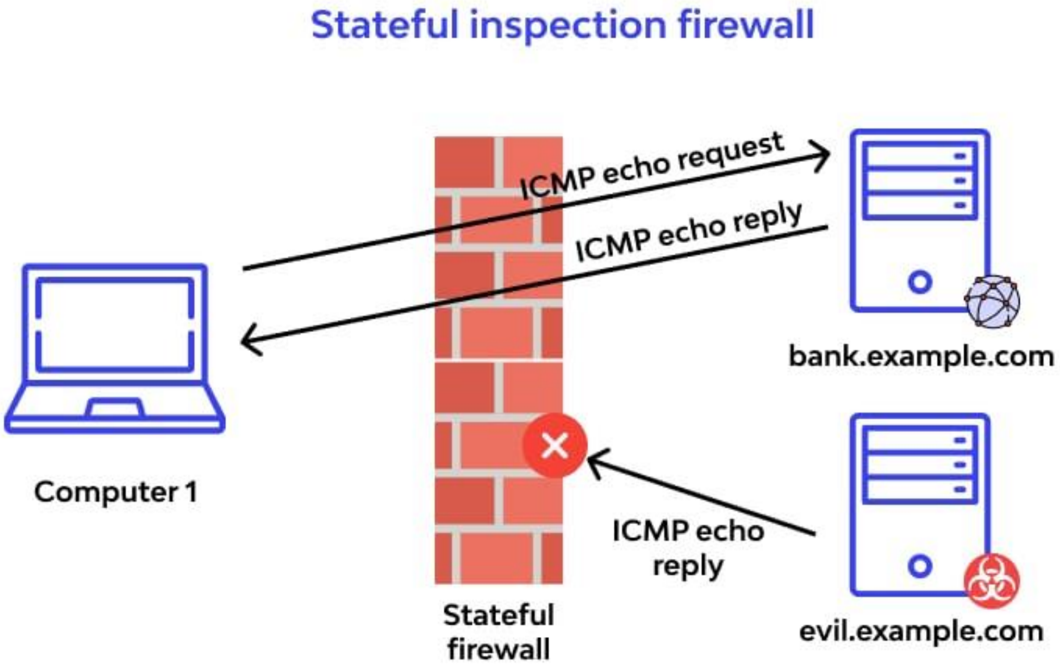
Flexibility: They can be configured to allow or deny traffic based on various criteria, including Ip addresses, ports, and sequence numbers.

WEAKNESSES:

Performance impact: The connection tracking feature introduces additional overhead, which may affect firewall performance, especially in high-traffic environments.

Limited application-layer inspection: Stateful firewalls do not deeply inspect application-layer protocols, which may leave certain application-specific vulnerabilities undetected.

Susceptible to DoS attacks: Stateful firewalls can be vulnerable to resource exhaustion attacks when dealing with a large number of concurrent connections.



APPLICATION-LAYER FIREWALL:

Application-layer firewalls, also known as proxy firewalls, operate at the application layer [Layer 7] of the OSI model. They provide the highest level of security by examining and filtering traffic based on the content and behavior of application-layer protocols

STRENGTHS:

Deep packet inspection: Application-layer firewalls can thoroughly inspect the payload of packets, enabling them to detect and prevent sophisticated attacks, such as SQL injection and cross-site scripting (XSS).

• Protocol awareness: They have in-depth knowledge of various application protocols, allowing them to enforce specific security policies tailored to individual applications.

•Enhanced security features: Application-layer Firewalls often include additional security features like content filtering, antivirus scanning, and intrusion detection/prevention systems.

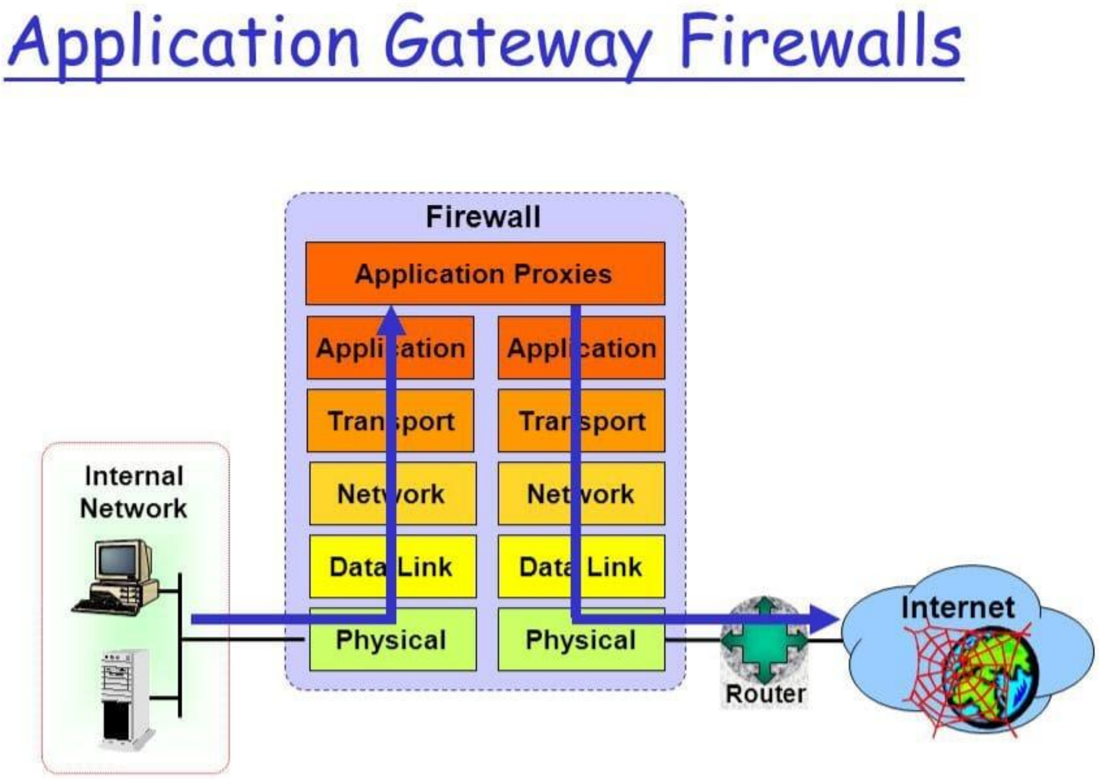
WEAKNESSES:

• Performance overhead: The intensive inspection and processing of application-layer traffic can significantly impact firewall performance and introduce latency, particularly in high-throughput environments.

•Complexity: Application-layer firewalls are more complex to configure and maintain compared to packet-filtering or stateful firewalls.

• Resource requirements: Their advanced features may require more computational resources

and memory, making them more expensive to implement.



Application Gateway Firewalls