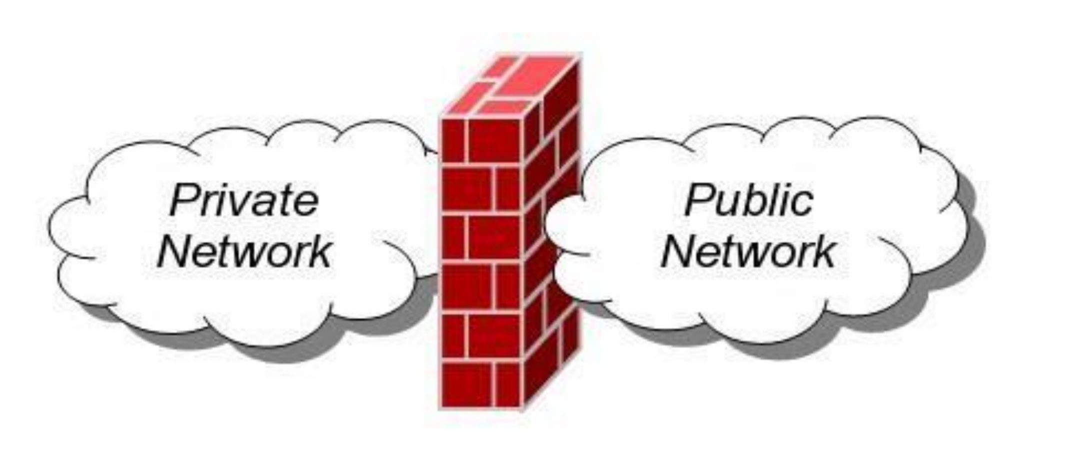
# Firewall Technologies

# What Is a Firewall ?

- **Definition**: A Network Firewall is a system or group of systems used to control access between two networks -- a trusted network and an untrusted network -- using pre-configured rules or filters.



# What Is a Firewall ?

It is the combination of hardware and software the method to access the network in an organization from the large internet world ,it allows the network administrator to control acess between the outside world and resourses within the network by managing the traffic flow from and to the resourses.

# Goals of Firewall ?

- All traffic from outside to inside ,and vice versa,passes through the firewall
- Only autorized traffic as defined by the local security policy will be allowed to pass.
- The firewall itself is resistant to penetration.

# Types of Firewalls

1. **By the Firewalls** methodology **:**

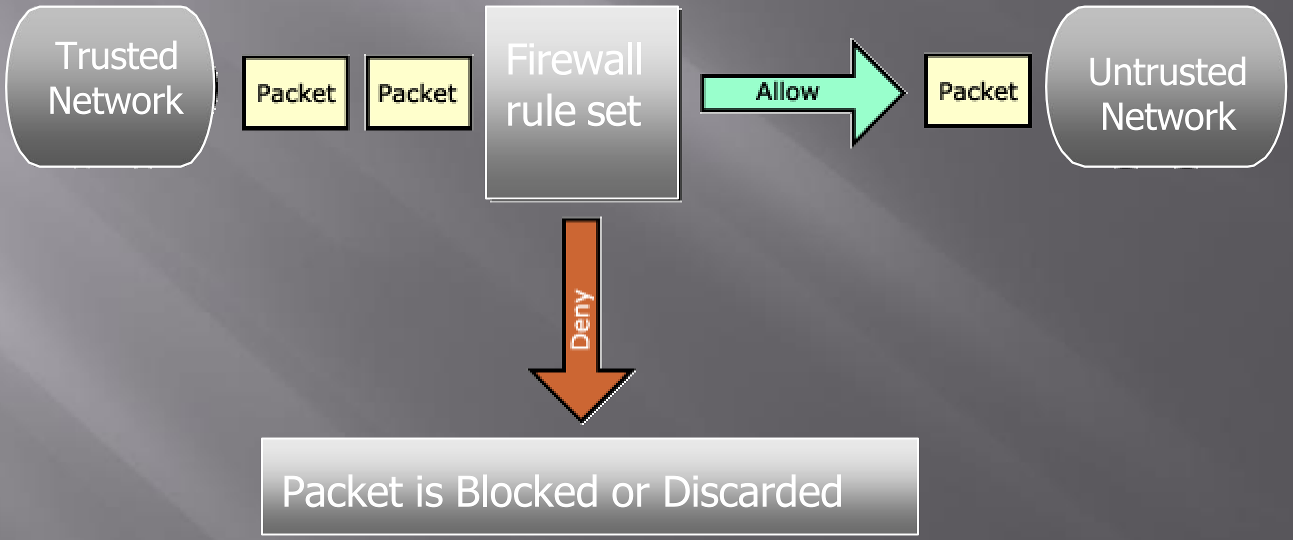
- Packet Filtering
- Stateful Packet Inspection
- Application Gateways/Proxies

# Packet Filtering Firewall

- As each packet passes through the firewall, it is examined and information contained in the header is compared to a pre-configured set of rules or filters. An allow or deny decision is made based on the results of the comparison. Each packet is examined individually without regard to other packets that are part of the same connection.

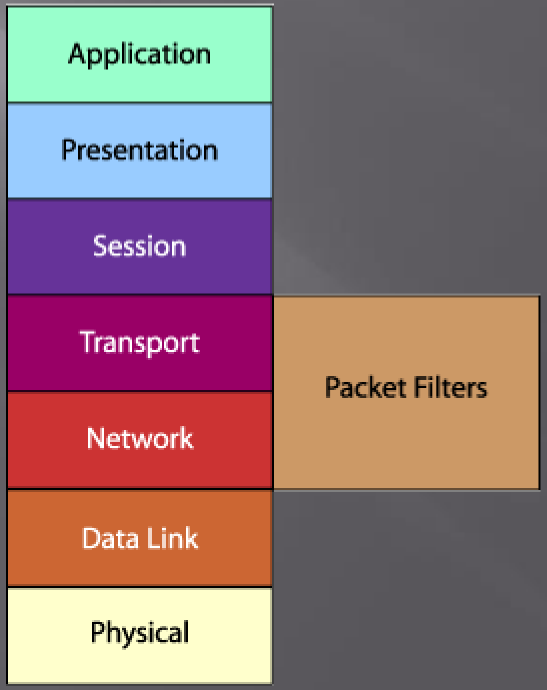
# Packet Filtering Firewall

**Packet Filtering Firewall**



# Packet Filtering Firewall

- A packet filtering firewall is often called a network layer firewall because the filtering is primarily done at the network layer (layer three) or the transport layer (layer four) of the OSI reference model.



# Packet Filtering Firewall

Packet filtering rules or filters can be configured to allow or deny traffic based on one or more of the following variables:

- Source IP address
- Destination IP address
- Protocol type (TCP/UDP)
- Source port
- Destination port

# Packet Filtering

- **Strengths :**
  - Packet filtering is typically faster than other packet screening methods. Because packet filtering is done at the lower levels of the OSI model, the time it takes to process a packet is much quicker.
  - Packet filtering firewalls can be implemented transparently. They typically require no additional configuration for clients.
  - Packet filtering firewalls are typically less expensive. Many hardware devices and software packages have packet filtering features included as part of their standard package.

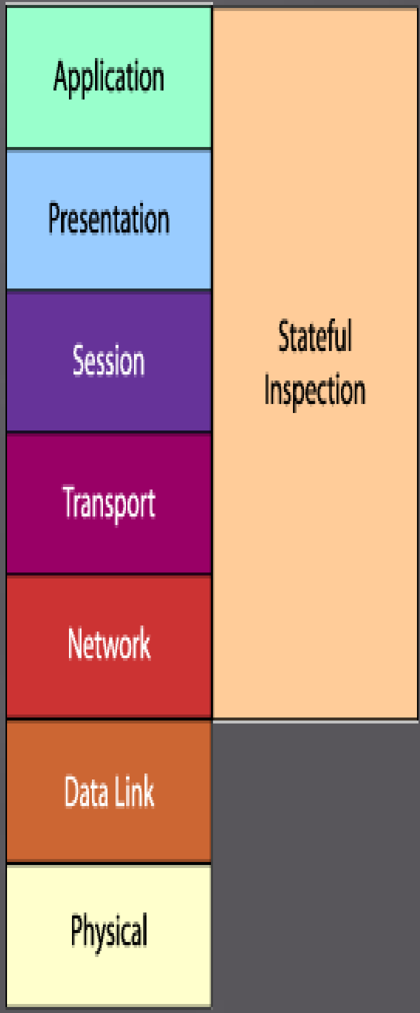
# Packet Filtering

**Weaknesses**

- Lack of authentication
- Defining rules and filters on a packet filtering firewall can be a complex task.

# Stateful Packet Inspection

- Stateful packet inspection uses the same fundamental packet screening technique that packet filtering does. In addition, it examines the packet header information from the network layer of the OSI model to the application layer to verify that  the packet is part of a legitimate connection and the protocols are behaving as expected.



Application

Presentation

Session

Transport

Network

Data Link

Physical

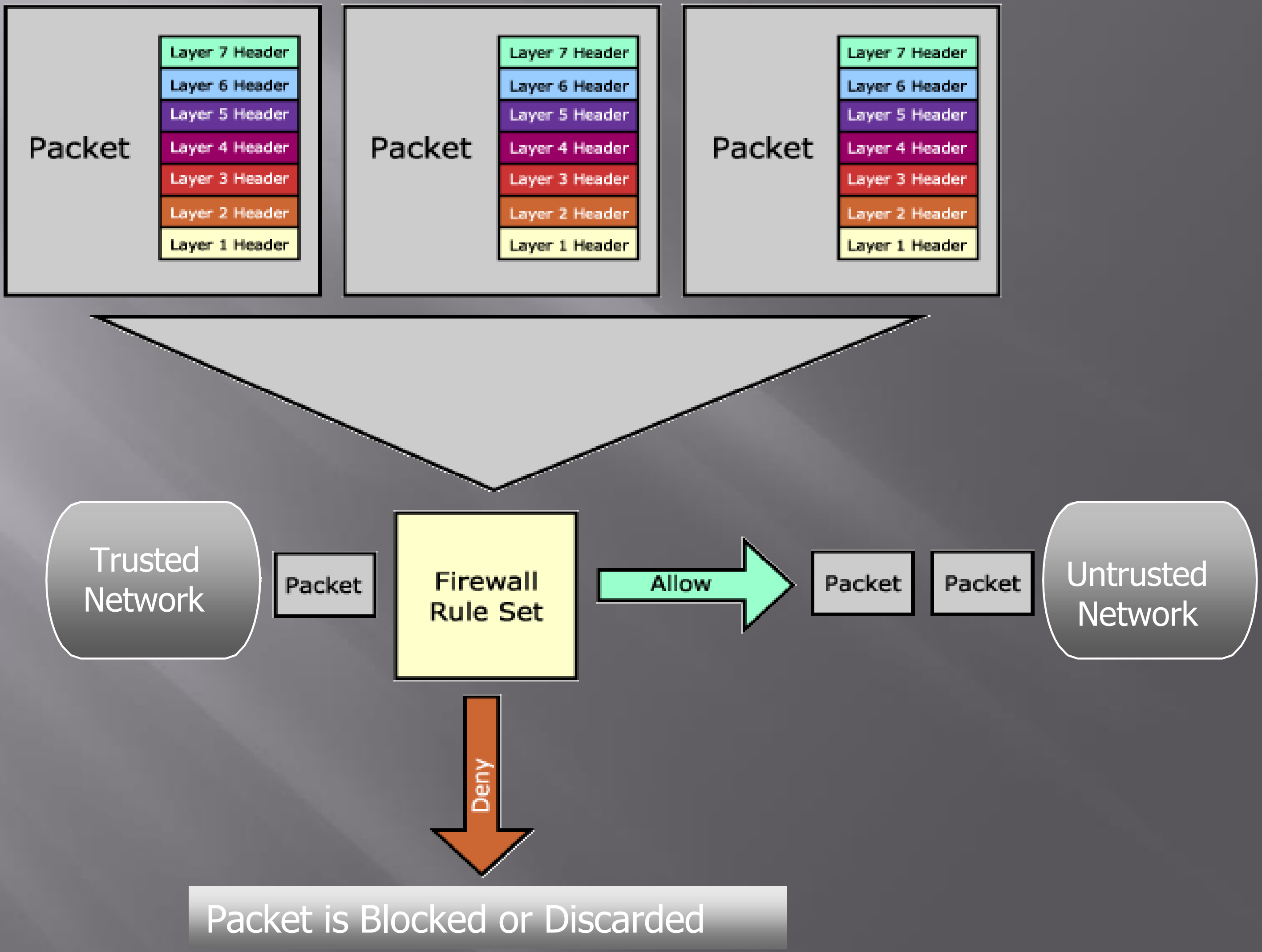
Stateful Inspection

# Stateful Packet Inspection Firewall

As packets pass through the firewall, packet header information is examined and fed into a dynamic state table where it is stored. The packets are compared to pre-configured rules or filters and allow or deny decisions are made based on the results of the comparison.

The data in the state table is then used to evaluate subsequent packets to verify that they are part of the same connection.

# Stateful Packet Inspection Firewall



# Stateful Packet Inspection

**Strengths :**

- More secure than basic packet filtering firewalls. Because stateful packet inspection digs deeper into the packet header information to determine the connection state between endpoints.
- Usually it have some logging capabilities. Logging can help identify and track the different types of traffic that pass though the firewall.

# Stateful Packet Inspection

**Weaknesses**

- Like packet filtering, stateful packet inspection does not break the client/server model and therefore allows a direct connection to be made between the two endpoints

- Rules and filters in this packet screening method can become complex, hard to manage, prone to error and difficult to test.

# Application Gateways/Proxies

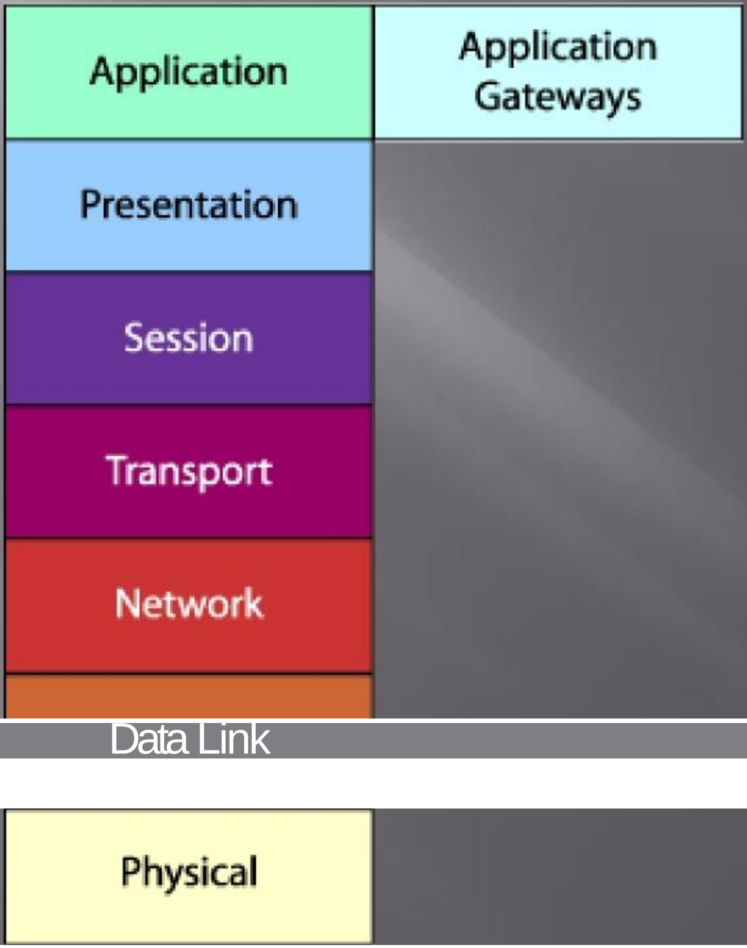
- The proxy plays middleman in all connection attempts.
- The application gateway/proxy acts as an intermediary between the two endpoints. This packet screening method actually breaks the client/server model in that two connections are required: one from the source to the gateway/proxy and one from the gateway/proxy to the destination. Each endpoint can only communicate with the other by going through the gateway/proxy.

# Application Gateways/Proxies

- This type of firewall operates at the application level of the OSI model. For source and destination endpoints to be able to communicate with each other, a proxy service must be implemented for each application protocol.

- The gateways/proxies are carefully designed to be reliable and secure because they are the only connection point between the two networks.

# Application Gateways/Proxies



Application

Application Gateways

Presentation

Session

Transport

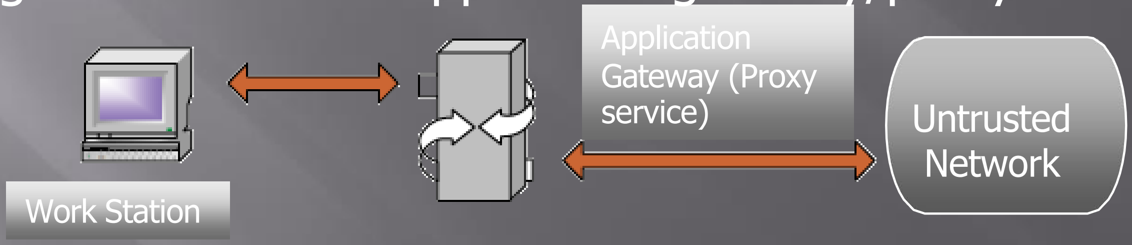
Network

Data Link

Physical

# Application Gateways/Proxies Firewall

- When a client issues a request from the untrusted network, a connection is established with the application gateway/proxy. The proxy determines if the request is valid (by comparing it to any rules or filters) and then sends a new request on behalf of the client to the destination. By using this method, a direct connection is never made from the trusted network to the untrusted network and the request appears to have originated from the application gateway/proxy.



# Application Gateways/Proxies Firewall

- The response is sent back to the application gateway/proxy, which determines if it is valid and then sends it on to the client.
- By breaking the client/server model, this type of firewall can effectively hide the trusted network from the untrusted network.
- It is important to note that the application gateway/proxy  only copying known acceptable commands before sending it on to the destination.

# Application Gateways/Proxies

**Strengths**

- Application gateways/proxies do not allow a direct connection to be made between endpoints. They actually break the client/server model.

- Allow the network administrator to have more control over traffic passing through the firewall. They can permit or deny specific applications or specific features of an application.

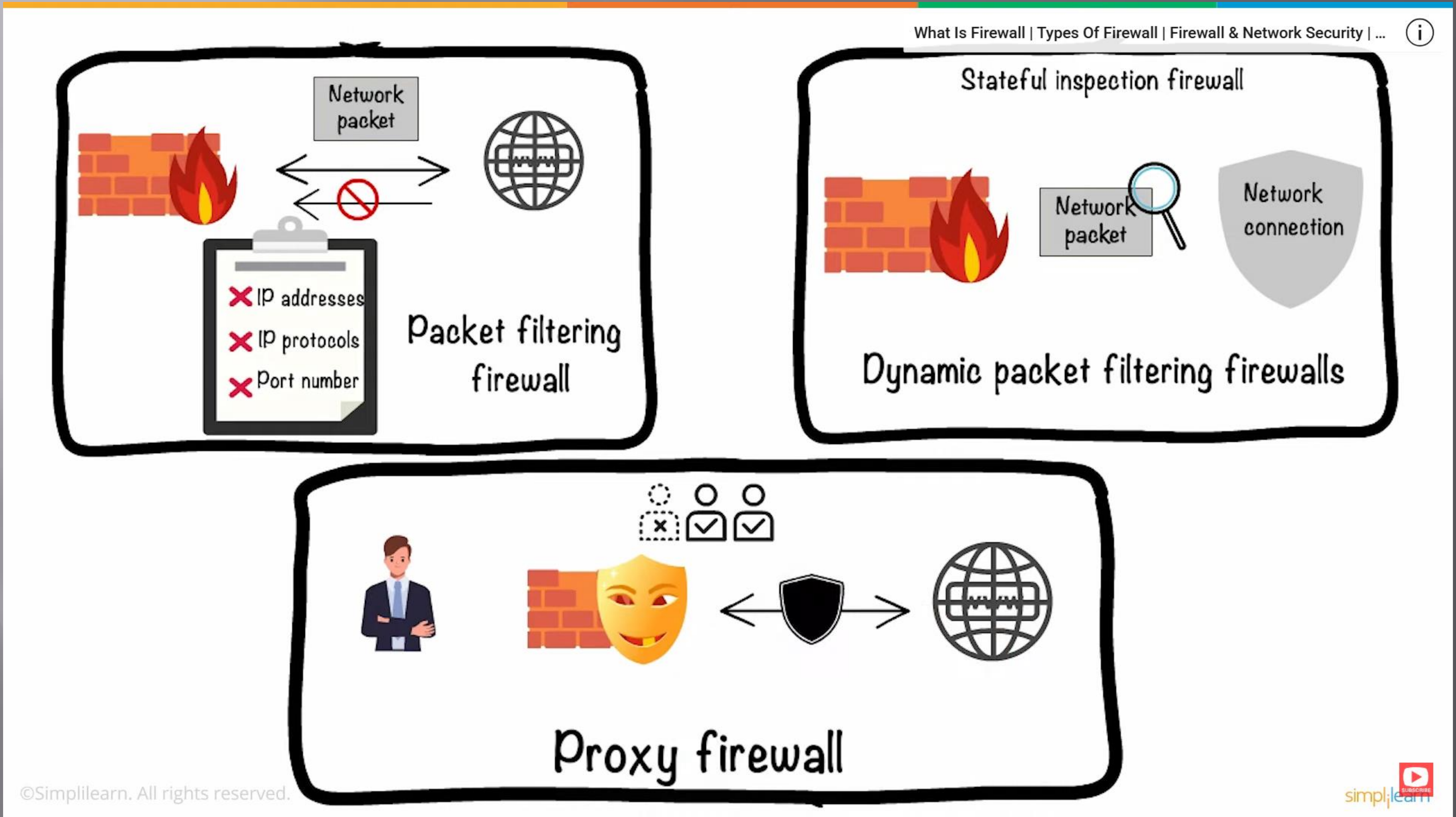
# Application Gateways/Proxies

**Weaknesses**

- The most significant weakness is the impact they can have on performance.

  it requires more processing power and has the potential to become a bottleneck for the network.

- Typically require additional client configuration. Clients on the network may require specialized software or configuration changes to be able to connect to the application gateway/proxy.



What Is Firewall | Types Of Firewall | Firewall & Network Security | ...