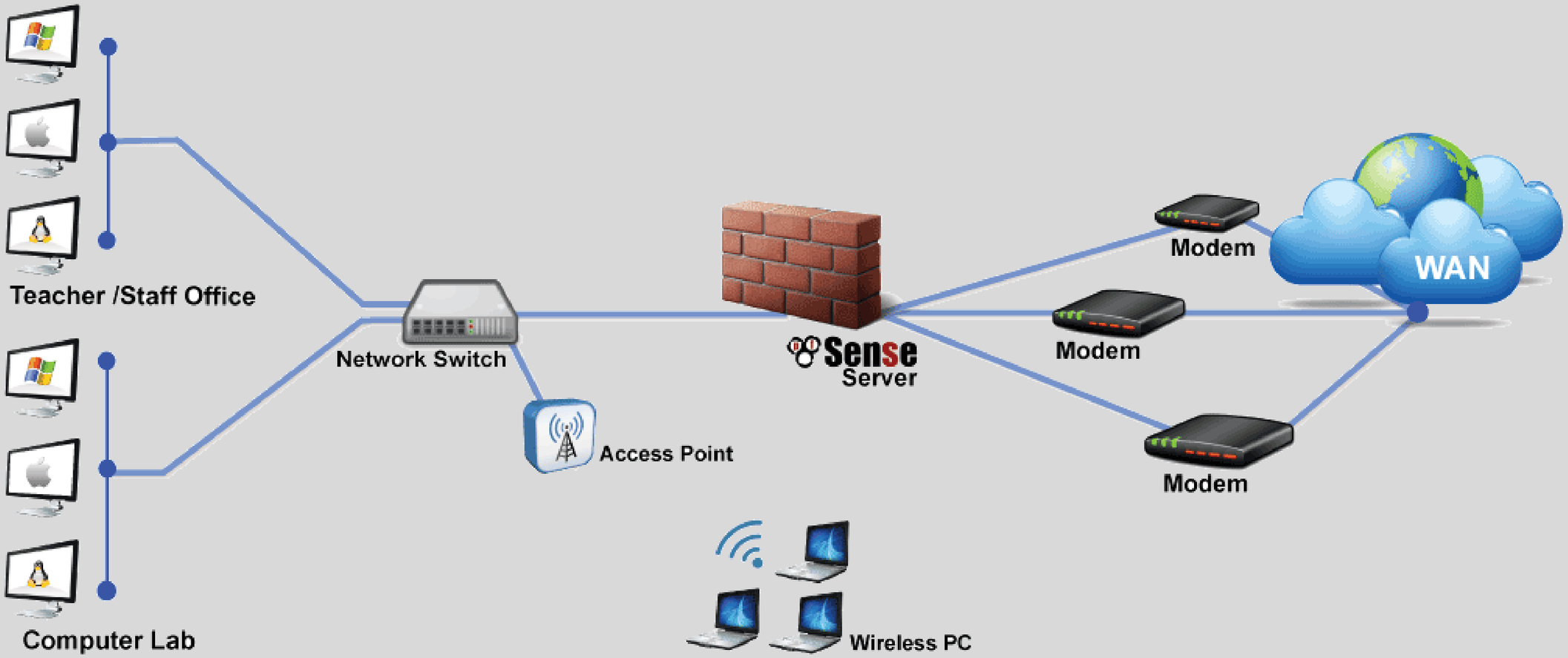
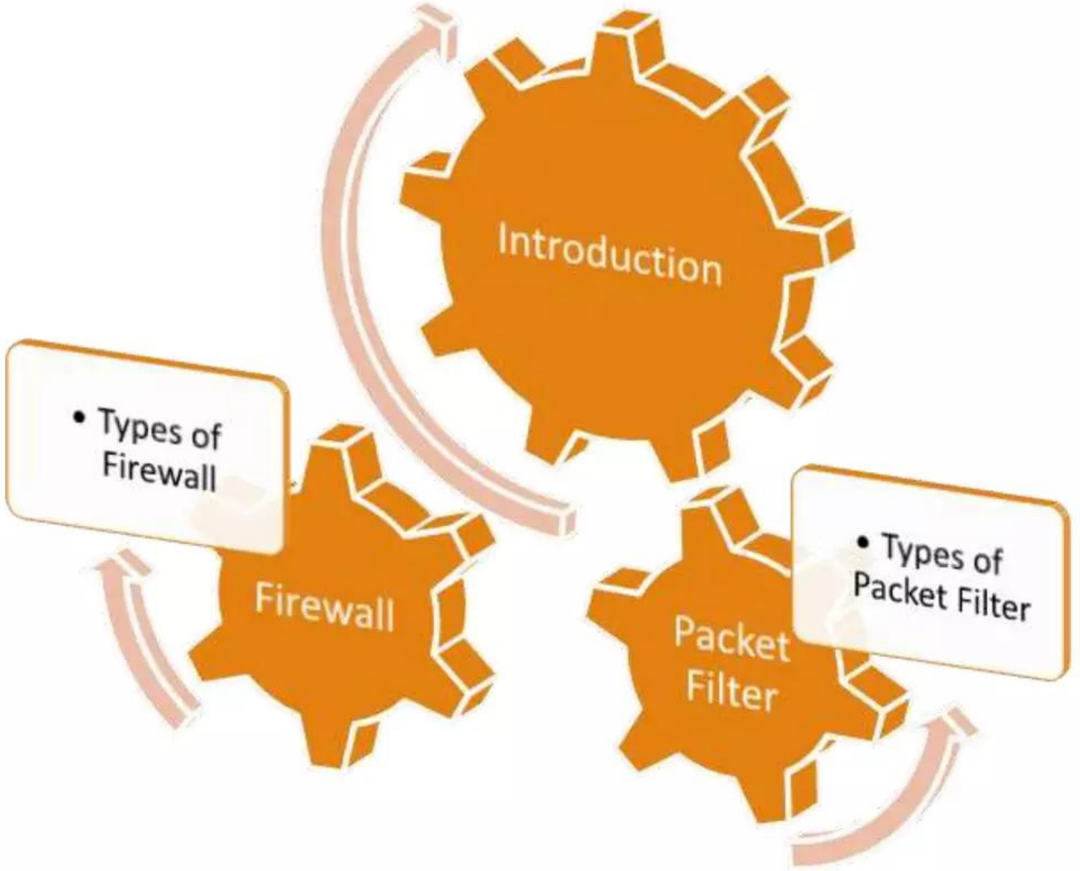
FIREWALLS AND PACKET FILTERS

PREPARED BY:

S.PRAKASH


Teacher /Staff Office
Computer Lab
Network Switch
Access Point
Sense
Server
Modem
Modem
Modem
WAN
Wireless PC

CONTENTS


Introduction
• Types of Firewall
Firewall
Packet Filter
• Types of Packet Filter

INTRODUCTION

Firewall is a network device that isolates organization’s internal network from larger outside network/Internet, it can be a hardware, software, or combined system.

Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol(IP) address, protocols and ports.

FIREWALL

A firewall is a protective system that lies, in between your computer network and the Internet. When used correctly, a firewall prevents unauthorized use and access to your network.

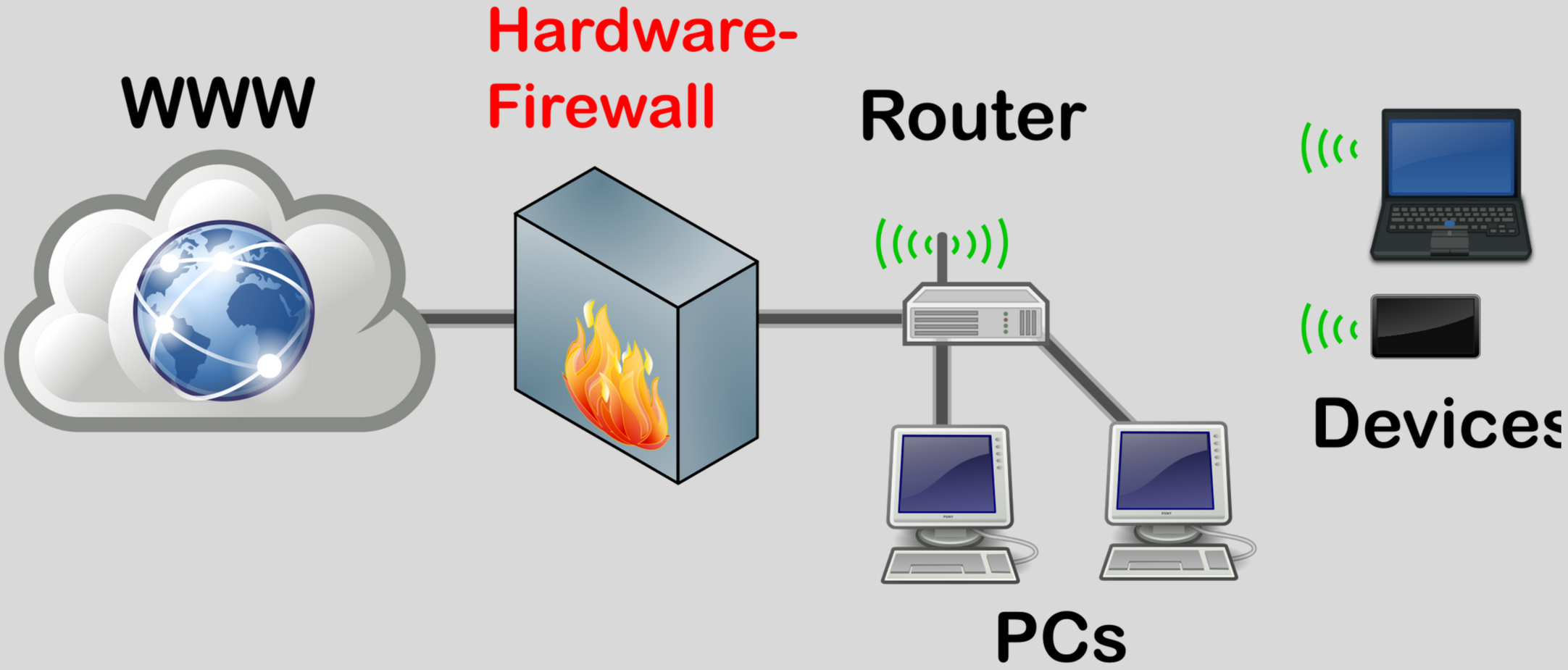
Hardware Firewalls

- Protect an entire network.
- Implemented on the router level.
- Usually more expensive, Harder to configure.

Software Firewalls

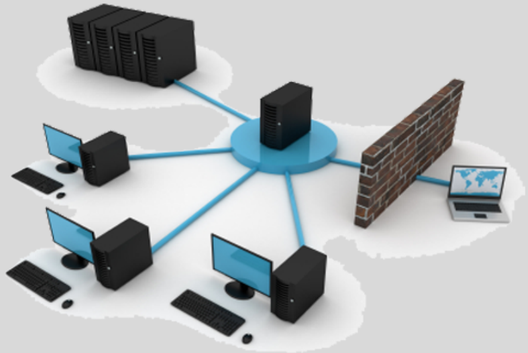
- Protect a single computer.
- Usually less expensive, Easier to configure.
- Most commonly used firewall.

HARDWARE FIREWALL

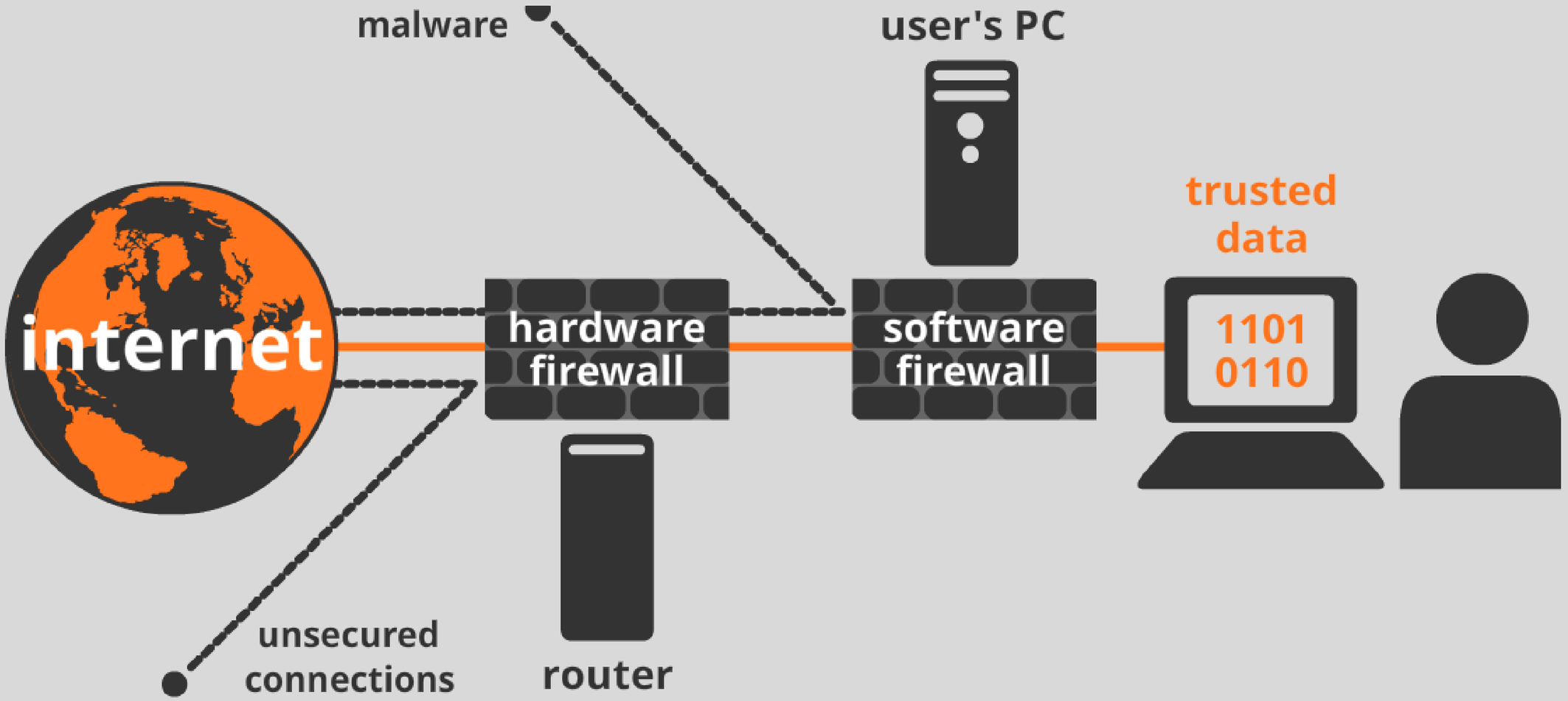


SOFTWARE FIREWALL

avast!



McAfee™
Together is power.

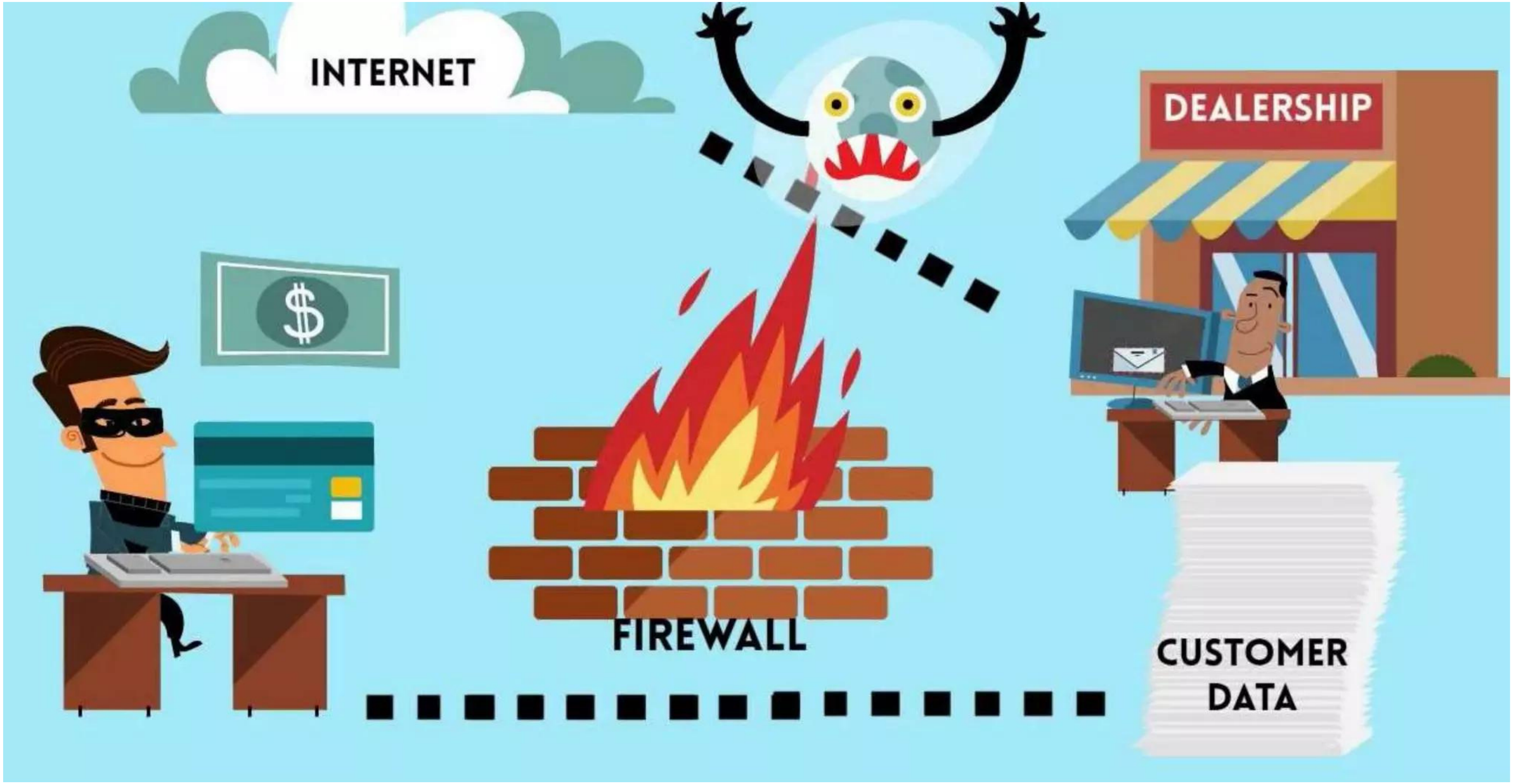

malware
user's PC
trusted
data
internet
hardware
firewall
software
firewall
1101
0110
unsecured
connections
router

HOW DOES FIREWALL WORK ?

A person/organization can program it to let what they want to get in and what they don't want to get out.

Inspects each individual "packet" of data as it arrives at either side of the firewall.

Determines whether it should be allowed to pass through or if it should be blocked.


INTERNET
DEALERSHIP
FIREWALL
CUSTOMER
DATA

ADVANTAGES

Focuses on security decisions

- Stop hackers from accessing your computer.

Can enforce security policy

- Protect your personal information.

Limits your exposure

- Blocks “Pop-Up” ads and certain cookies.

Can log internet activity efficiently

- Determines which programs can access the internet.

DISADVANTAGES

- Legitimate User Restriction
- Diminished Performance
- Can’t protect against Internal Attack
- Maintenance and configuration is difficult
- Weak against viruses, malwares, etc.

TYPES OF FIREWALL

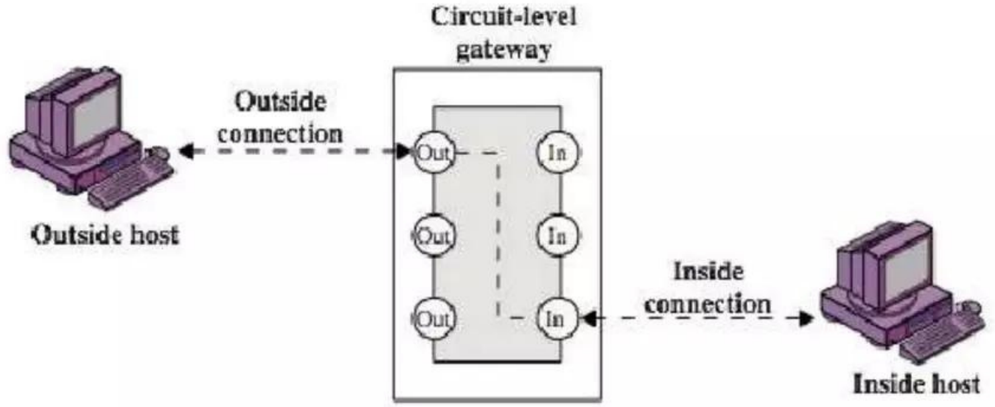
Application Proxy Firewall

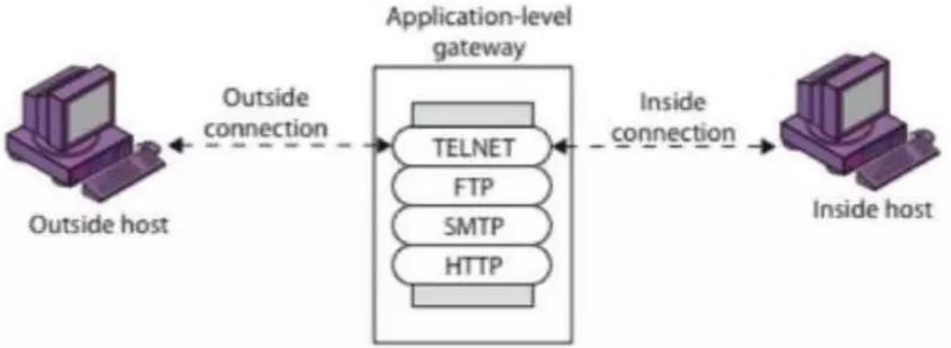
- A proxy firewall is a network security system that protects network resources by filtering messages at the application layer. A proxy firewall may also be called an application firewall or gateway firewall.

Circuit Level Firewall

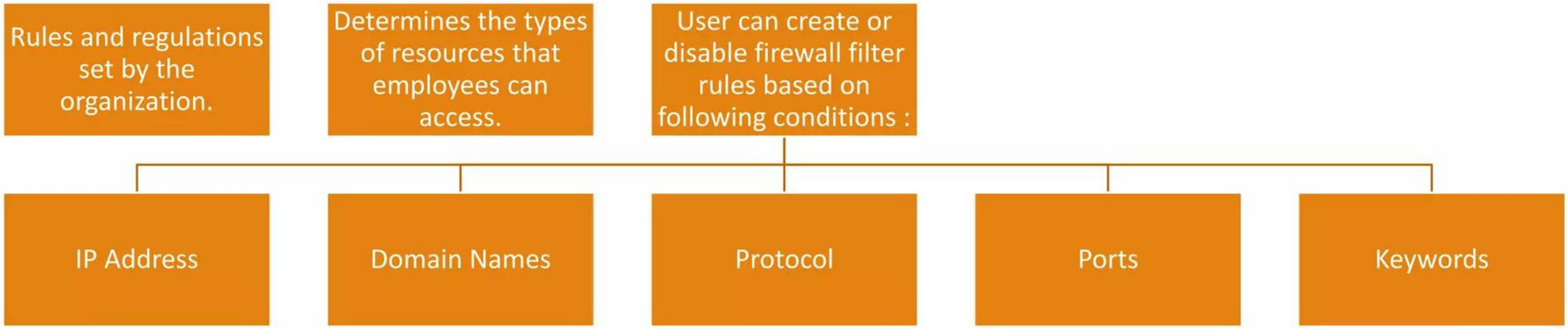
- A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security, and works between an Open Systems Interconnection (OSI) network model's transport and application layers such as the session layer.
- Unlike application gateways, circuit-level gateways monitor TCP data packet handshaking and session fulfillment of firewall rules and policies.

Packet Filter Firewall


Circuit-level gateway
Outside connection
Out
In
Out
In
Out
In
Inside connection
Outside host
Inside host


Application-level gateway
Outside connection
TELNET
FTP
SMTP
HTTP
Inside connection
Outside host
Inside host

FIREWALL RULES



PACKET FILTERS

Packet filter firewall controls access to packets on basis of packet source and destination address or specific transport protocol type.

During network communication, a node transmits a packet that is filtered and matched with predefined rules and policies. Once matched, a packet is either accepted or denied.

Packet filtering checks source and destination IP addresses. If both IP addresses match, the packet is considered secure and verified.

Because the sender may use different applications and programs, packet filtering also checks source and destination protocols, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

Packet filters also verify source and destination port addresses.

Advantages

- Low cost
- Low resource usage which in turn gives better performance
- Does not require user knowledge or co-operation

Disadvantages

- Testing and debugging are difficult
- Implementing rules is difficult
- Network topology is not hidden from attacker

TYPES OF PACKET FILTERS

Stateless firewalls watch network traffic and restrict or block packets based on source and destination addresses or other static values. They're not 'aware' of traffic patterns or data flows.

A stateless firewall uses simple rule-sets that do not account for the possibility that a packet might be received by the firewall 'pretending' to be something you asked for.

A stateless firewall filter, also known as an access control list (ACL), does not statefully inspect traffic. Instead, it evaluates packet contents statically and does not keep track of the state of network connections.

Stateless firewalls are typically faster than stateful firewalls and perform better under heavier traffic loads.

Stateful firewalls can watch traffic streams from end to end. They are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption.

In technical terms, this means that stateful firewalls can tell what stage a TCP connection is in (open, synchronized, synchronization acknowledge or established). It can tell if the MTU has changed and whether packets have fragmented, etc.

Stateful firewalls are better than stateless firewalls at identifying unauthorized and forged communications.

Thank you!