FIREWALL

INTRODUCTION

- Firewall is a cyber security tool that is used to filter traffic on a network.
- IT prevents intruders like virus, Trojans, ransomware, other types of malware and other such security threats from breaking into networks and infecting them.
- Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications.
- Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons.

TYPES OF FIREWALLS

- Packet filtering firewalls
- Application level gateways (proxy firewalls)
- Circuit level gateways
- Stateful inspection firewalls
- Next gen firewalls

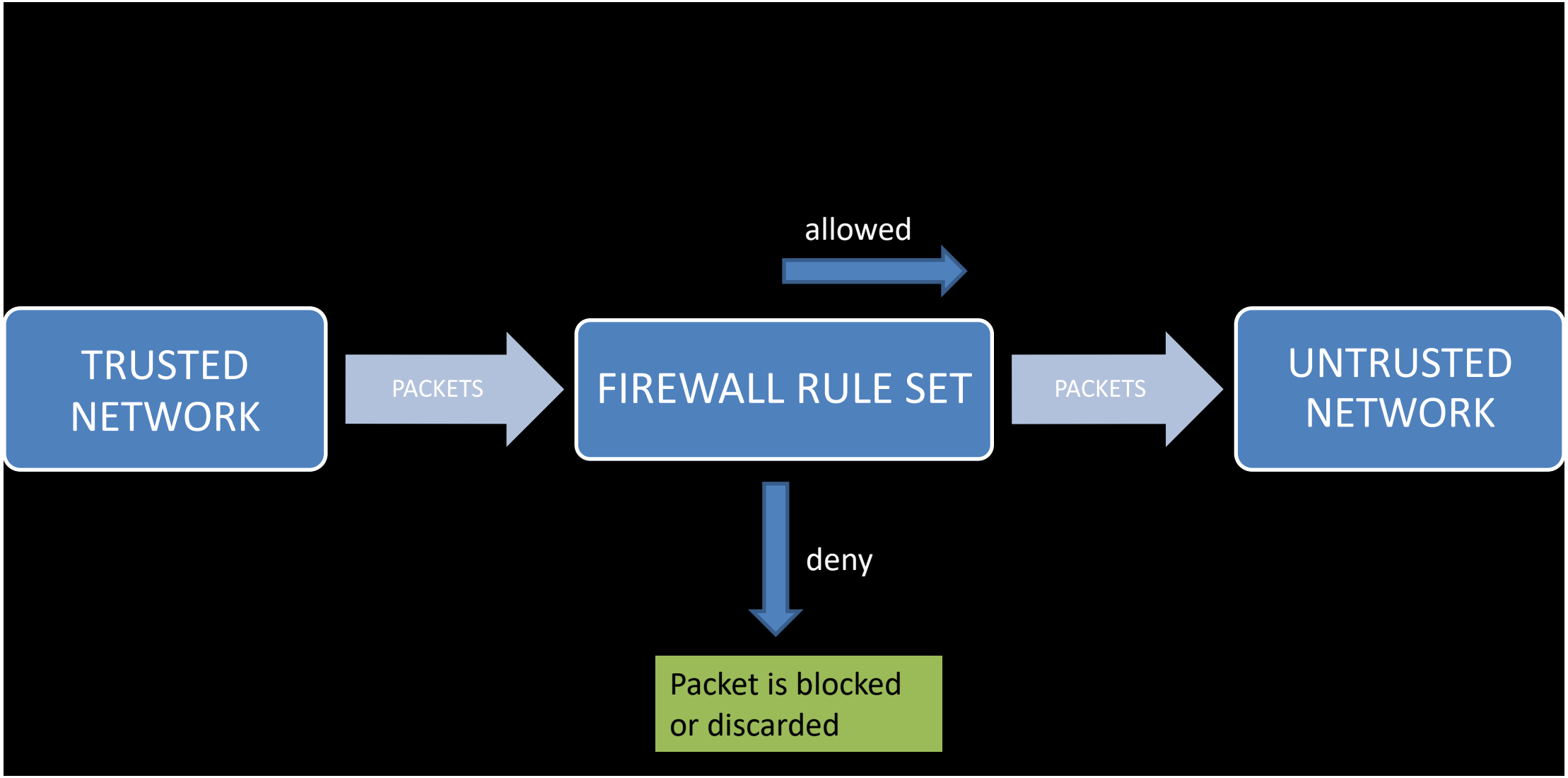
1. PACKET FILTERING FIREWALLS

- It works on the network layer of the OSI model.
- It is a hardware firewall.
- It creates checkpoint at router or switch.
- Simplest and less secure

WORKING

- A filtering table is created. It includes source IP address, destination IP address, protocols and ports.
- It applies the set of rules (based on the filtering table’s contents) on each packet and based on the outcome, decides to either forward or discard the packet.
- An organisation predefines all the rules so that only legitimate users can access their sensitive data.

WORKING


allowed
TRUSTED NETWORK
PACKETS
FIREWALL RULE SET
PACKETS
UNTRUSTED NETWORK
deny
Packet is blocked or discarded

SECURITY THREATS

- IP address spoofing : In this kind of attack, an intruder from the outside tries to send a packet towards the internal corporate network with the source IP address set equal to one of the IP address of the internal users.
- Source routing attacks : In it, the attacker specifies the route to be taken by the packet with a hope to fool the firewall.
- Tiny fragment attacks : In it, the attacker intentionally creates fragments of the original packets and send it to fool the firewall.

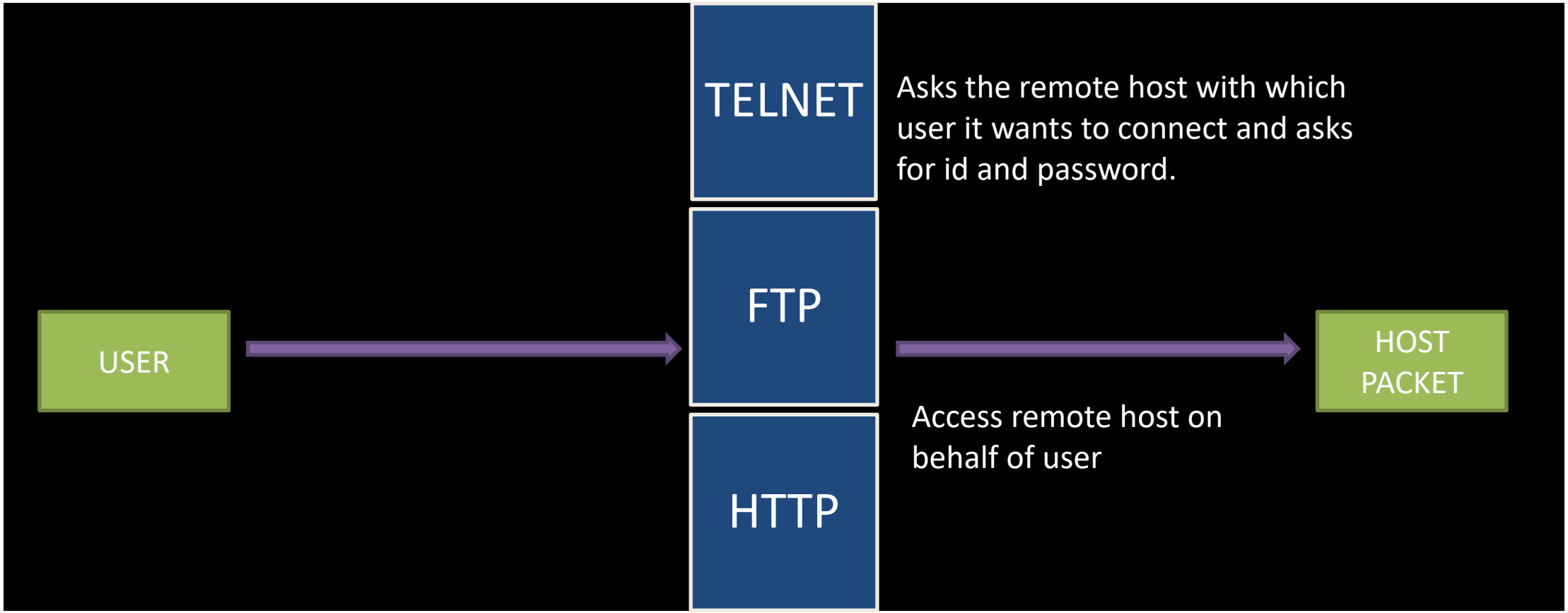
2. APPLICATION LEVEL GATEWAYS

- It works at the application layer of the OSI model.
- It is also known as proxy servers.
- It is more secure than packet filtering.

WORKING

- Step 1: User contacts the application gateways using a TCP/IP application such as http.
- Step 2: The application gateway asks about the remote hosts with which the user wants to establish a connection. It also asks for the user id and password to access the service of the application gateway.
- Step 3: After verifying the authenticity of the user, the application gateway access the remote host on behalf of the user to deliver the packets.

WORKING



APPLICATION GATEWAY
(PROXY SERVER)

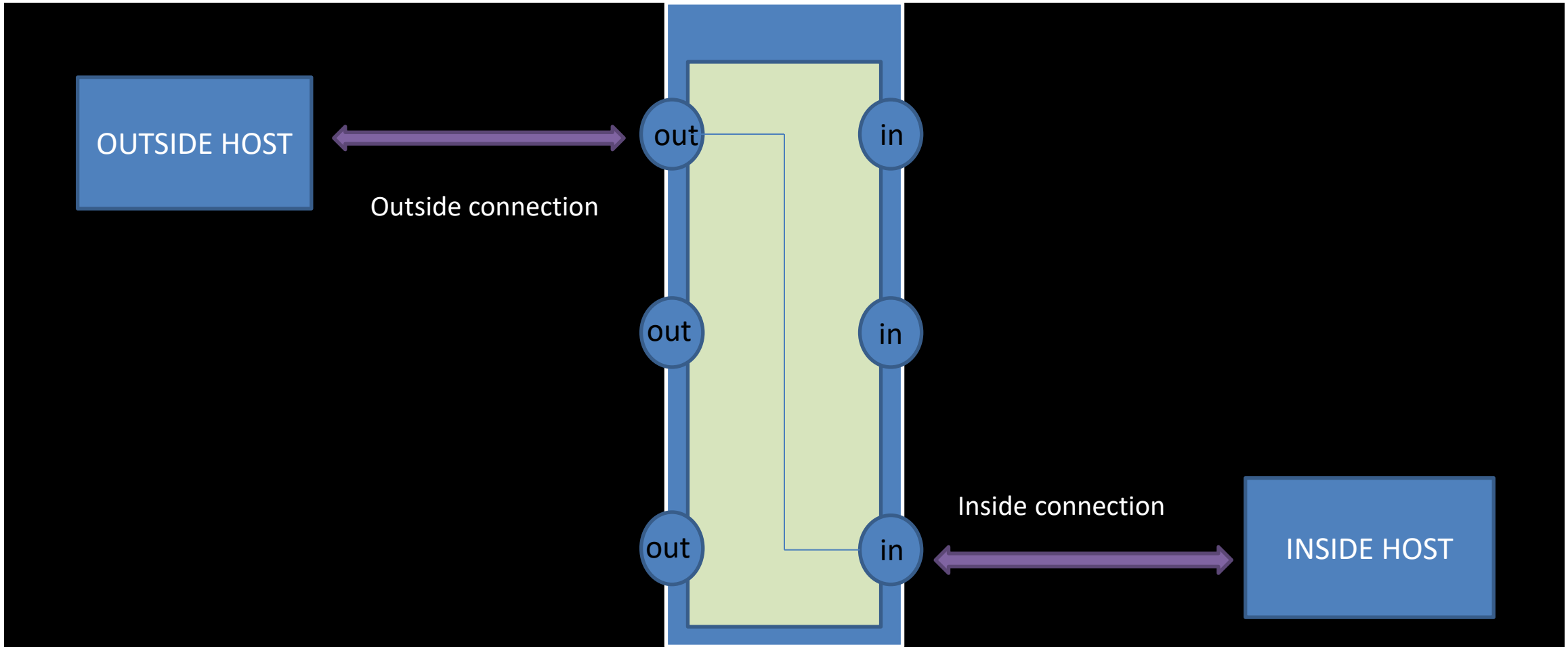
3. CIRCUIT LEVEL GATEWAYS

- It works at the session layer of the OSI model.
- It is the advanced variation of the application gateway.
- It acts as a virtual connection.
- Faster then application level gateways because there is less evaluation.
- Extremely resource-efficient
- Less secure

WORKING

- Circuit level gateways work by verifying the TCP handshakes. This TCP handshake check is designed to make sure that the packet is from the legitimate.
- It uses 2 TCP connections: between internal hosts and gateways between external hosts and gateways
- Security check is done before setting up the connection. If connection is established only then the data will be passed.

WORKING


OUTSIDE HOST
Outside connection
out
in
out
in
out
in
Inside connection
INSIDE HOST

4. STATEFUL INSPECTION

- These firewalls combine both packet inspection technology and TCP handshake verification.
- Very secure
- Utilizes more resources
- Packet transfer becomes slow

WORKING

- It keeps track of the state of active connections and uses this information to decide which packet to allow through it, i.e.,it adapts itself to the current exchange of information, unlike the normal packet/filters, which have hardcoded routing rules.
- It also keeps track of whether or not that packet is part of an established TCP or other network session.

5. NEXT GENERATION FIREWALL

Common features of next-gen firewalls:

- Deep packet inspection
- TCP handshake checks
- Surface level packet inspection
- Includes IPS(intrusion prevention systems)

WORKING

- Deep packet inspection looks at the actual data the packet is carrying unlike traditional packet inspection which looks at protocol header of the packet.
- A deep packet inspection firewall tracks the progress of the web browsing session and is capable of noticing whether a packet payload constitutes a legitimate html formatted response.

Thank you..