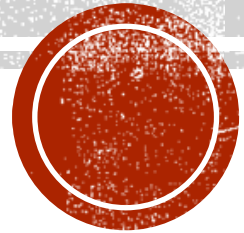
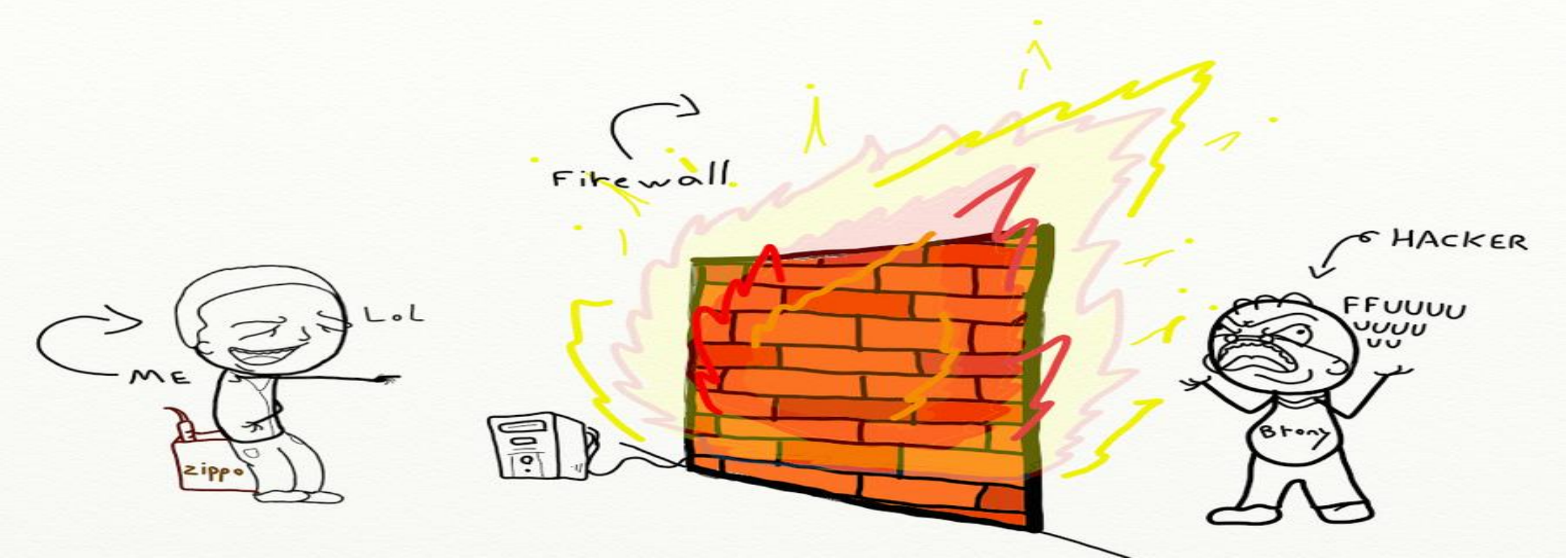
FIREWALLS



WHAT IS FIREWALL

- A Firewall is a software or hardware system designed to prevent unauthorized access to an individual computer or network of computers.
- Firewalls can be implemented as both hardware and software, or a combination of both. It's a part of almost all operating systems
- At its core, firewall examines traffic on a network interface to determine whether packets should be allowed to enter or leave the interface. Thus, firewall software blocks inbound connections to a system's services that shouldn't be exposed to other systems on a public network and can also be used to block outbound traffic from a system to a network.
- Firewalls block traffic to known malware sites to try and limit the potential damage of downloading an infected file.
- Firewalls take the direction of traffic into consideration when filtering packets. It uses two main categories of filters.

FIREWALL



HISTORY OF FIREWALLS

- 1988 – First Generation – Packet-Filter Firewall
- 1989 – Second Generation – Stateful Firewall
- 1991 – Third Generation – Application Layer Firewall
- 2004 – IDC coins the term Unified Threat Management (UTM)
- 2009 – Gartner defines the Next-Generation FireWall (NGFW).

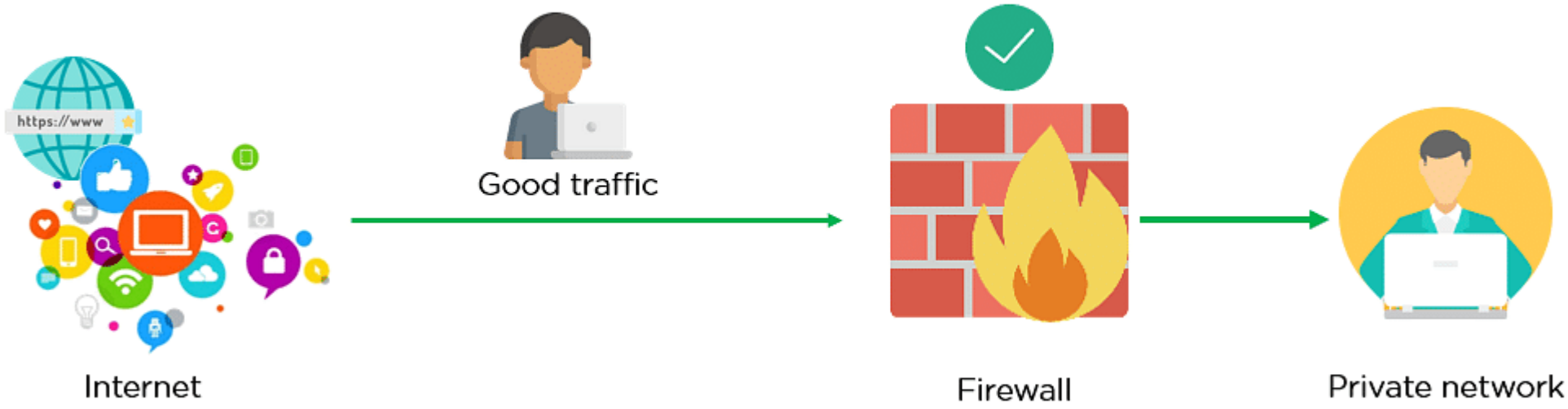
WHY WE USE FIREWALL

- Firewalls are network security systems that prevent unauthorized access to a network. It can be a hardware or software unit that filters the incoming and outgoing traffic within a private network, according to a set of rules to spot and prevent cyberattacks.
- Firewalls are designed with modern security techniques that are used in a wide range of applications.
- In the early days of the internet, networks needed to be built with new security techniques, especially in the client-server model, a central architecture of modern computing.
- That's where firewalls have started to build the security for networks with varying complexities. Firewalls are known to inspect traffic and mitigate threats to the devices.

KEY USE OF FIREWALL

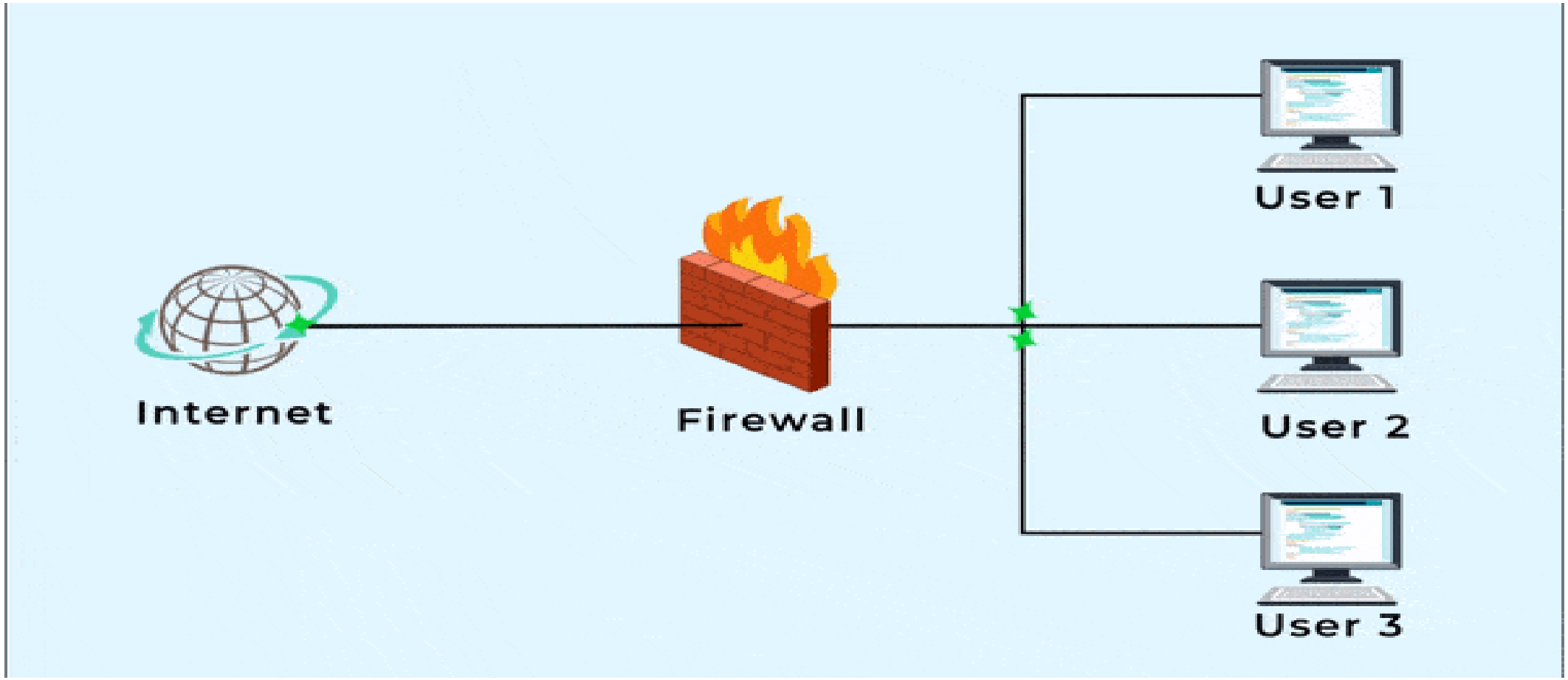
- Firewalls can be used in corporate as well as consumer settings.
- Firewalls can incorporate a security information and event management strategy (SIEM) into cybersecurity devices concerning modern organizations and are installed at the network perimeter of organizations to guard against external threats as well as insider threats.
- Firewalls can perform logging and audit functions by identifying patterns and improving rules by updating them to defend the immediate threats.
- Firewalls can be used for a home network, Digital Subscriber Line (DSL), or cable modem having static IP addresses. Firewalls can easily filter traffic and can signal the user about intrusions.
- They are also used for antivirus applications.
- When vendors discover new threats or patches, the firewalls update the rule sets to resolve the vendor issues.
- In-home devices, we can set the restrictions using Hardware/firmware firewalls

HOW DOSE FIREWALL WORK?

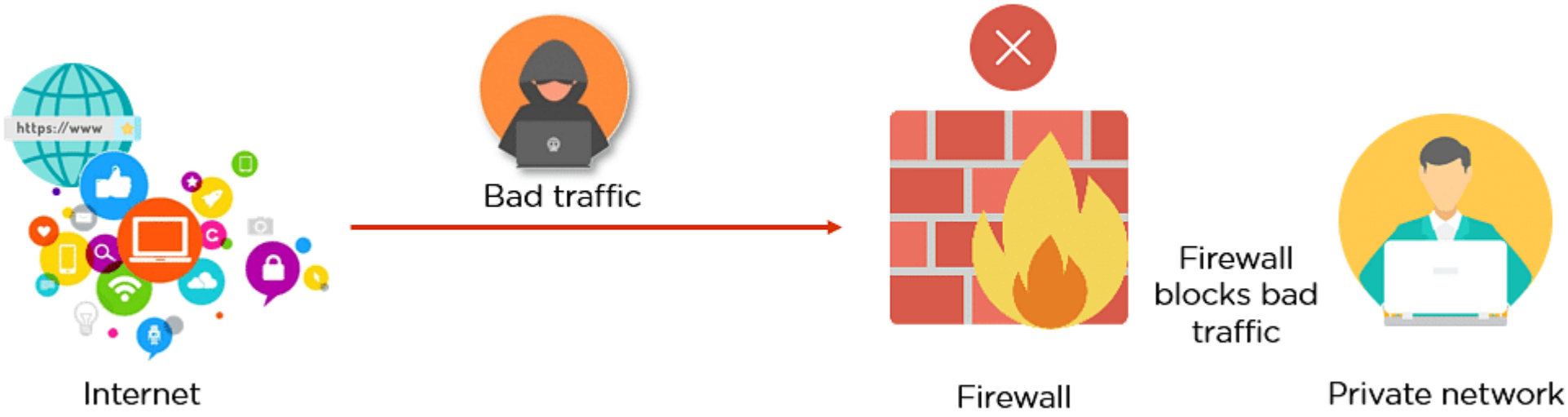


Firewall allowing Good Traffic

GOOD FIREWALL TRAFFIC

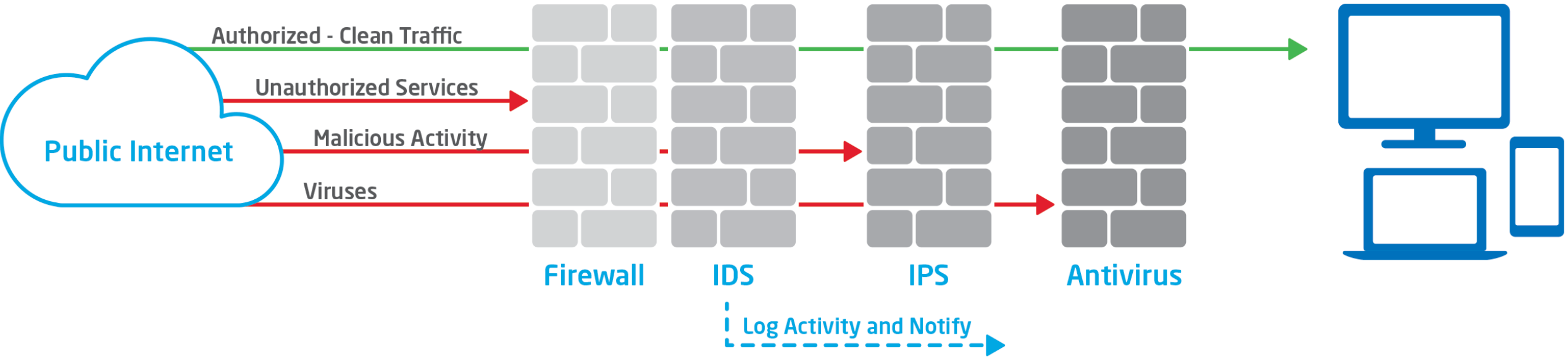


CONT...



Firewall blocking Bad Traffic

CONT...


Authorized - Clean Traffic
Unauthorized Services
Malicious Activity
Viruses
Public Internet
Firewall
IDS
IPS
Antivirus
Log Activity and Notify

TYPES OF FIREWALLS

- There are multiple types of firewalls based on their traffic filtering methods, structure, and functionality. A few of the types of firewalls are:
  - Packet Filtering
  - Proxy Service Firewall
  - Stateful Inspection
  - Next-Generation Firewall
  - Unified Threat Management (UTM) Firewall
  - Threat-Focused NGFW

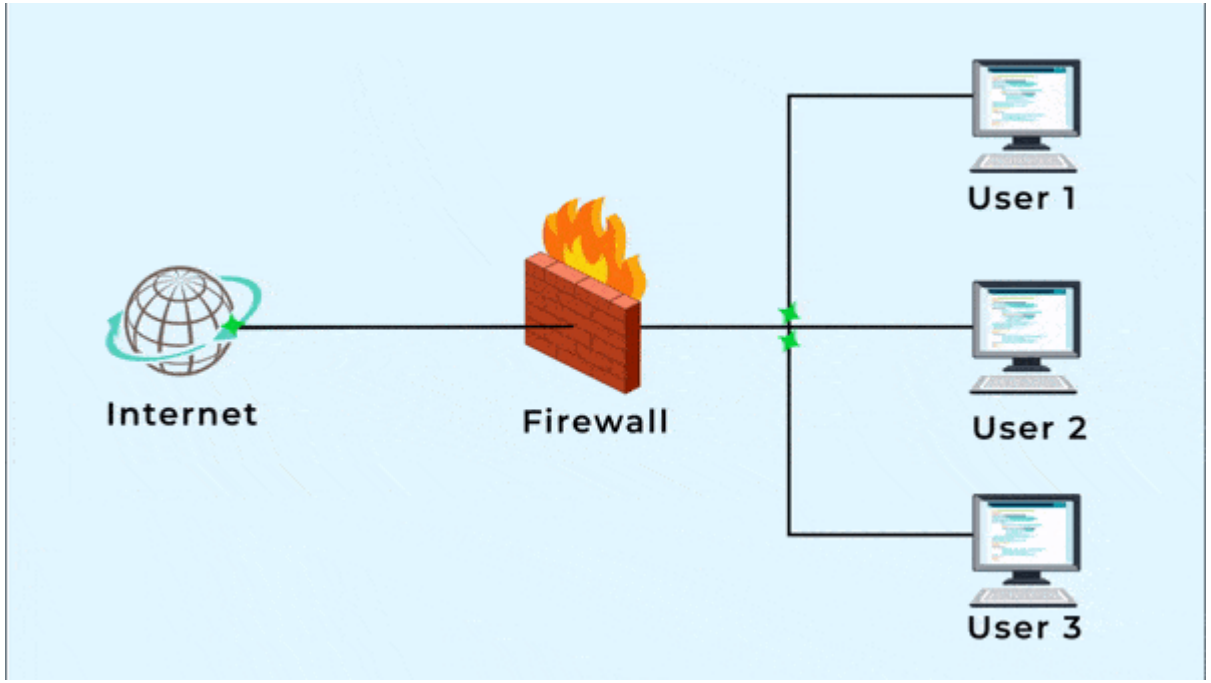
ADVANTAGES OF FIREWALL

- Firewalls play an important role in the companies for security management. Below are some of the important advantages of using firewalls.
- It provides enhanced security and privacy from vulnerable services. It prevents unauthorized users from accessing a private network that is connected to the internet.
- Firewalls provide faster response time and can handle more traffic loads.
- A firewall allows you to easily handle and update the security protocols from a single authorized device.
- It safeguards your network from phishing attacks.

HOW TO USE FIREWALL PROTECTION

- Constantly update your firewalls as soon as possible: Firmware patches keep your firewall updated against any newly discovered vulnerabilities.
- Use antivirus protection: In addition to firewalls, you need to use antivirus software to protect your system from viruses and other infections.
- Limit accessible ports and host: Limit inbound and outbound connections to a strict whitelist of trusted IP addresses.
- Have active network: To avoid downtime, have active network redundancies. Data backups for network hosts and other critical systems can help you avoid data loss and lost productivity in the case of a disaster.

HOW FIREWALL STOPS BAD REQUEST



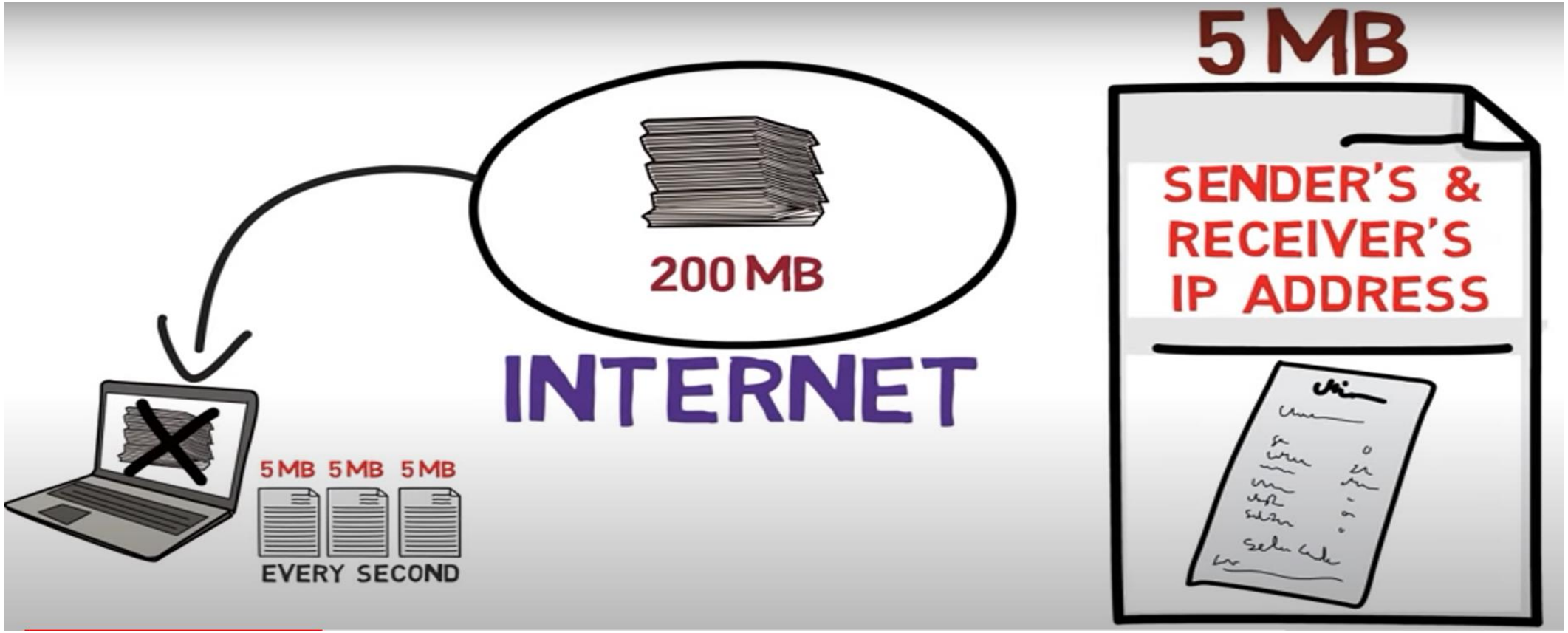
WHAT IS PACKET FILTER

- Data travels on the internet in small pieces; these are called packets. Each packet has certain metadata attached, like where it is coming from(source IP), where it should be sent to(destination IP) on which port it should be connected etc..
- A packet filter examines each datagram in isolation, determining whether the datagram should be allowed to pass or should be dropped based on administrator-specific rules.
- 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) addresses, protocols and ports.

PACKET FILTERING

- A packet filtering firewall controls data flow to and from a network. It allows or blocks the data transfer based on the packet's source address, the destination address of the packet, the application protocols to transfer the data, and so on.

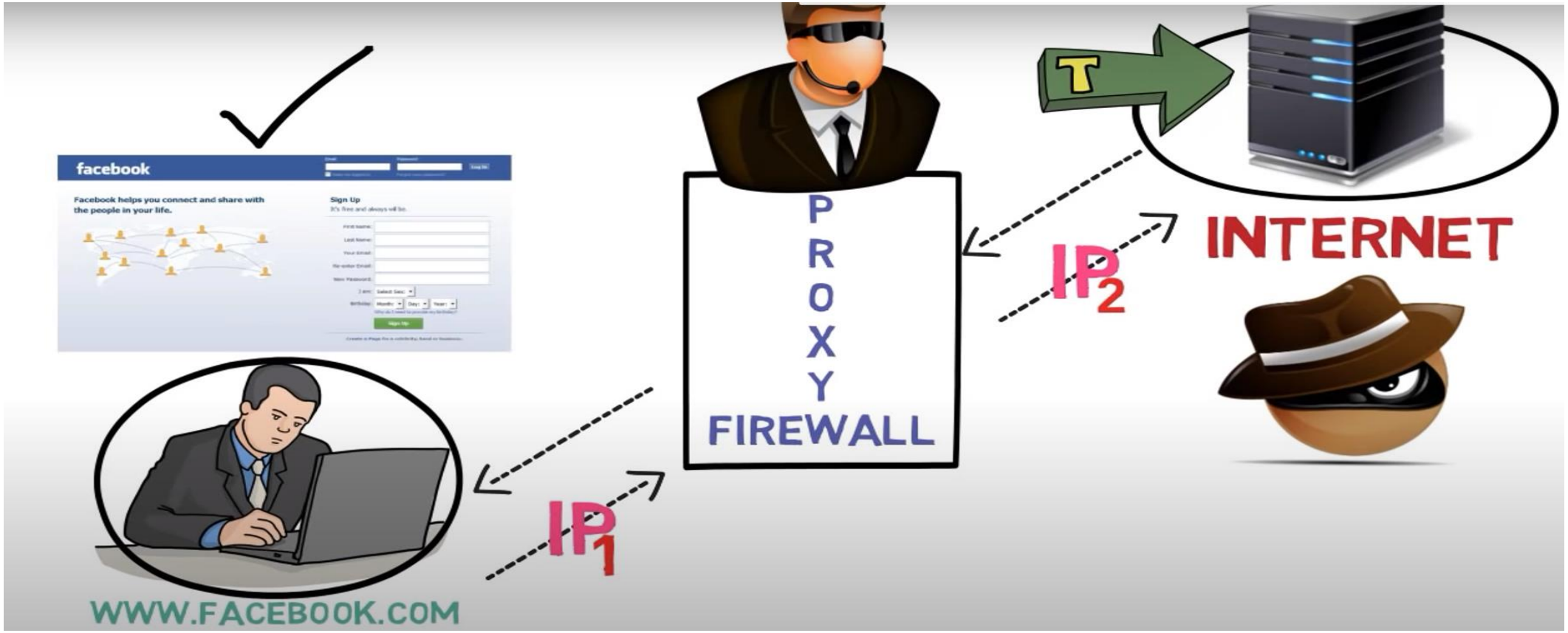
PACKET FILTERING



PROXY FIREWALL

- This type of firewall protects the network by filtering messages at the application layer. For a specific application, a proxy firewall serves as the gateway from one network to another.

PROXY FIREWALL



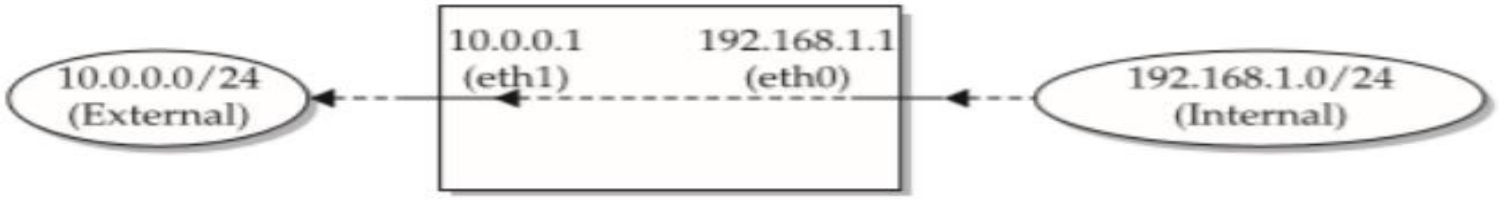
PACKET CHARACTERISTIC TO FILTER

- Most firewalls and packet filters have the ability to examine the following characteristics of network traffic:
- Type of protocol (IP, TCP, UDP, ICMP, IPSec, etc.)
- Source IP address and port
- Destination IP address and port
- ICMP message type and code
- TCP flags (ACK, FIN, SYN, etc.)
- Network interface on which the packet arrives

EXAMPLE

- if we wanted to block incoming ping packets (ICMP echo requests) to our home network of 192.168.1.0/24, we can write something like the following rule.
  - **deny proto icmp type 8:0 from any to 192.168.1.0/24**
- The important components of the rule are the action (deny), the packet attributes (ICMP protocol, specifically "ping" types), the direction of the rule (packets "from" one source "to" another), and the type of source (a network address range like 192.168.1.0/24).
- Example2:
- Imagine a firewall's external interface (called eth1) has an IP address of 10.0.0.1 with a netmask of 255.255.255.0.
- The firewall's internal interface (called eth0) has an IP address of 192.168.1.1 with a netmask of 255.255.255.0.

- Any traffic from the 192.168.1.0 network destined to the 10.0.0.0 network will come in to the eth0 interface and go out of the eth1 interface as shown in the diagram below



Conversely, traffic from the 10.0.0.0/24 network destined for the 192.168.1.0/24 network will come in to the eth1 interface and go out of the eth0 interface.

- Therefore, traffic with a source address in the 192.168.1.0/24 range coming inbound on the eth1 interface should be be never seen. If we see that, it means someone on the external 10.0.0.0/24 network is attempting to spoof an address in our local IP range.

- The firewall can stop this kind of activity by using a rule like the following:
  - deny proto any from 192.168.1.0/24 to any on eth1
- The above rule may be ambiguous. It might match the legitimate traffic coming from 192.168.1.0/24 heading out to the external network. It could, but it depends on the firewall's interpretation of the syntax.
- We can rewrite the rule with less ambiguity by specifying the network interface on which it should be applied as follows
- **deny proto any from 192.168.1.0/24 to any in on eth1**
- **allow proto any from 192.168.1.0/24 to any out on eth1**
- We have to be very careful when writing firewall rules. Simply knowing what we are trying to block isn't sufficient, we must verify that the rule works as expected.

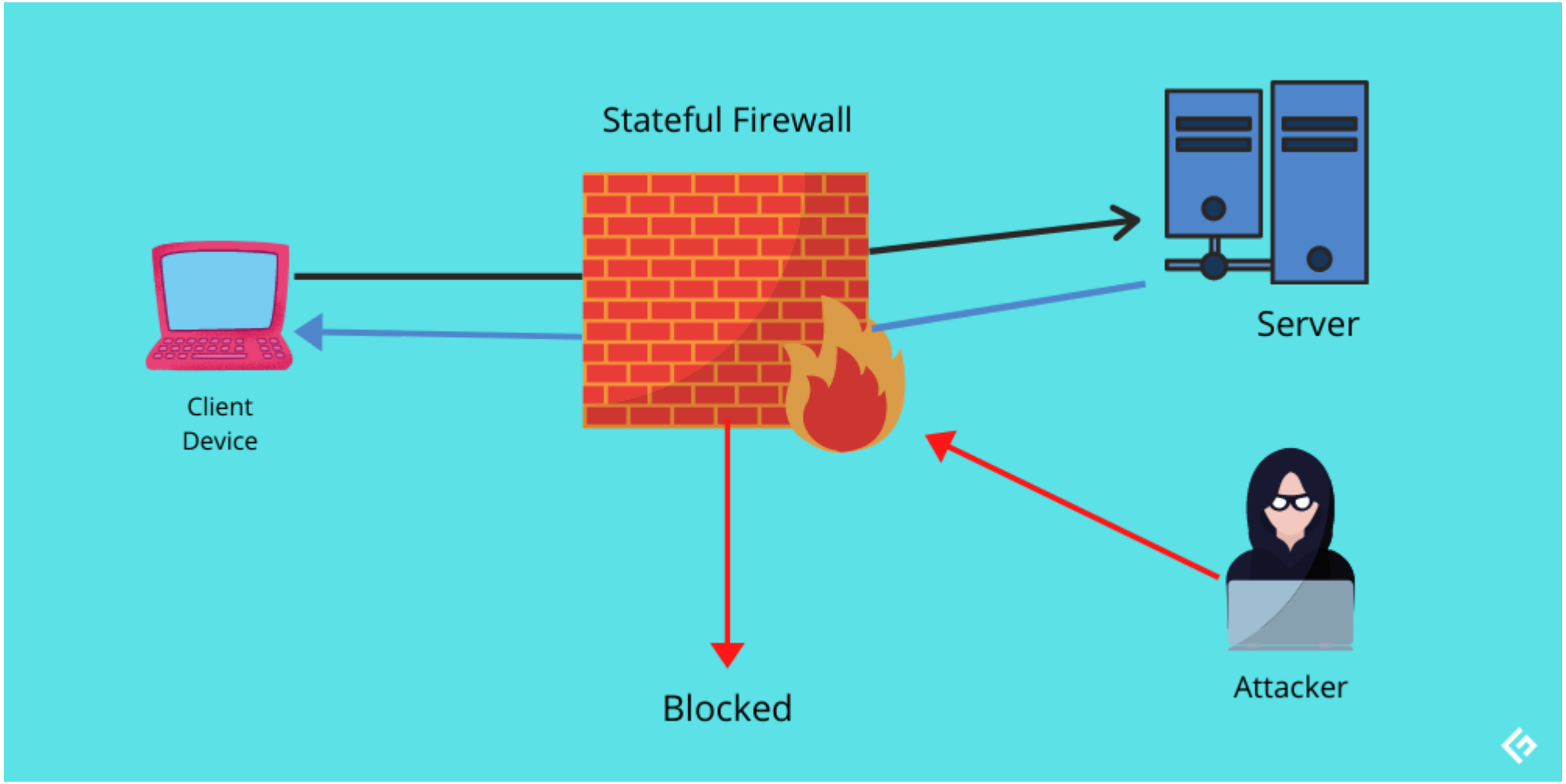
STATELESS VS STATEFUL FIREWALLS

- A stateless firewall examines individual packets in isolation from each other. It doesn't track whether related packets have arrived before or are coming after.
- A stateful firewall places that packet in the context of related traffic and within a particular protocol, such as TCP/IP or FTP. This enables stateful firewalls to group individual packets together into concepts like connections, sessions, or conversations.
- A stateful firewall is able to filter traffic based not only on a packet's characteristics, but also on the context of a packet according to a session or conversation.
- For example, a TCP ACK packet will be denied if the protected service hasn't set up the SYN and SYN-ACK handshake to establish a connection.
- Stateful firewalls also allow for more dynamic rulesets.

STATEFUL FIREWALL

- Stateful firewalls are capable of monitoring all aspects of network traffic, including their communication channels and characteristics.
- They are also referred to as dynamic pocket filters as they filter traffic packets based on the context and state.
- Now, what do these **context** and **state** mean in the language of network connections?
- **Context** – it involves metadata of packets including ports and IP address belonging to the endpoint's and destination, packet length, layer 3 information related to reassembly and fragmentation, flags, and numbers for TCP sequence of layer 4, and more.
- **State** – firewalls apply their policy based on the state of the connection. To understand the state, let's take the example of TCP-based communication. In TCP, 4 bits control connection state – SYN, ACK, FIN, and RST.
- When a connection initiates through a 3-way handshake, then the TCP indicates the SYN flag, which the firewall uses to indicate the arrival of a new connection. Next, the connection receives the flag SYN+ACK by the server. Until the client reverts with ACK, the connection does not establish.

STATEFUL FIREWALL



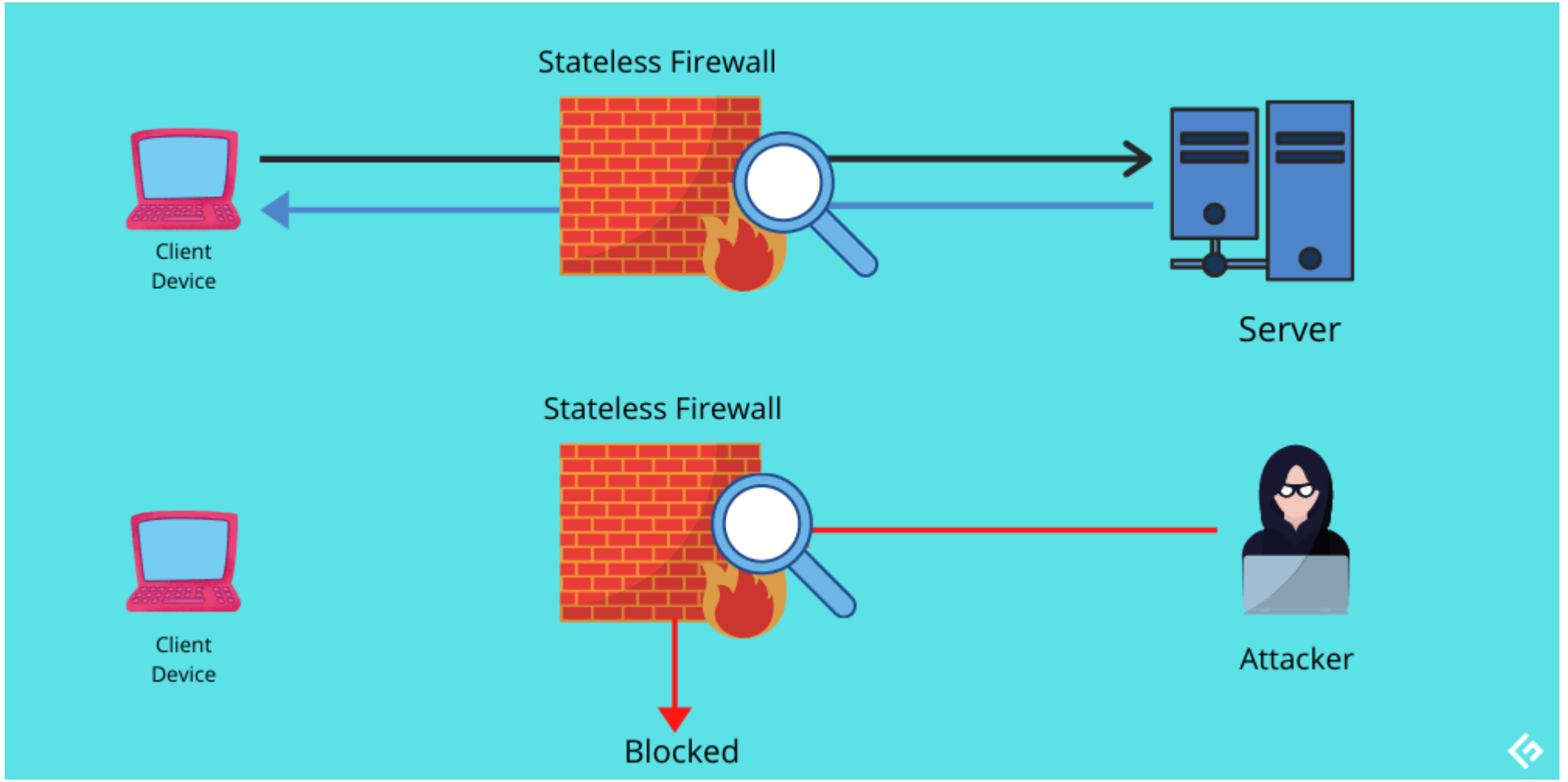
BENEFITS

- Powerful memory to retain key aspects of traffic
- Highly skilled to detect forged messaging or unauthorized access
- Intelligent system to make better decisions based on present and past findings
- Wider logging capacity and stronger attack mitigation
- Needs lesser ports for communication
- It implies that stateful firewalls keep on analyzing every data packet trying to enter into a network. Once the stateful firewall approves a traffic request, it can travel freely inside the network.
- However, stateful firewalls can be vulnerable to DDoS attacks. The reason behind the same is the increased need for software-network connection and intense computational power for implementation.

STATELESS FIREWALL

- Stateless firewalls utilize clues from key values like source, destination address, and more to check whether any threat is present. On detecting a possible threat, the firewall blocks it. There are certain preset rules that firewalls enforce while deciding whether traffic must be permitted or not.
- As stateless firewalls are not designed to consider as many details as stateful firewalls, they are less rigorous.
- For example, a stateless firewall cannot take into account the complete pattern in which packets are entering. Instead, it will inspect each packet in isolation. Furthermore, it also fails to differentiate between different traffic types of application-level, including HTTPS, HTTP, SSH, FTP, VolP, etc.
- Consequently, stateless firewalls are susceptible to online attacks spread across different packets.

STATELESS FIREWALL



BENEFITS

- Performs well in case of heavy traffic
- Fast
- Generally, cheaper than stateful firewalls.
- **Note**:
- Example of stateful and stateless firewall
  - **Small businesses**
  - **Enterprises**

  - A stateless firewall does not inspect entire traffic or packet and can’t identify traffic types.

NETWORK ADDRESS TRANSLATION (NAT)

- Networking devices are the gateways between networks. They separate external networks like the Internet from private networks like those used by the systems in our home.
- Systems on the Internet must have unique, public (i.e., "routable") IP addresses. This ensures that packets for a web site or a gaming server always go to the right destination.
- Internal networks, on the other hand, use "non-routable" IP addresses, referred to as private or RFC 1918 addresses.
- The Internet Assigned Numbers Authority (IANA) reserved those IP address blocks for private networks.
- This enables organizations large and small to build networks whose traffic will not leak onto the Internet unless it passes through a gateway device like a router or firewall.

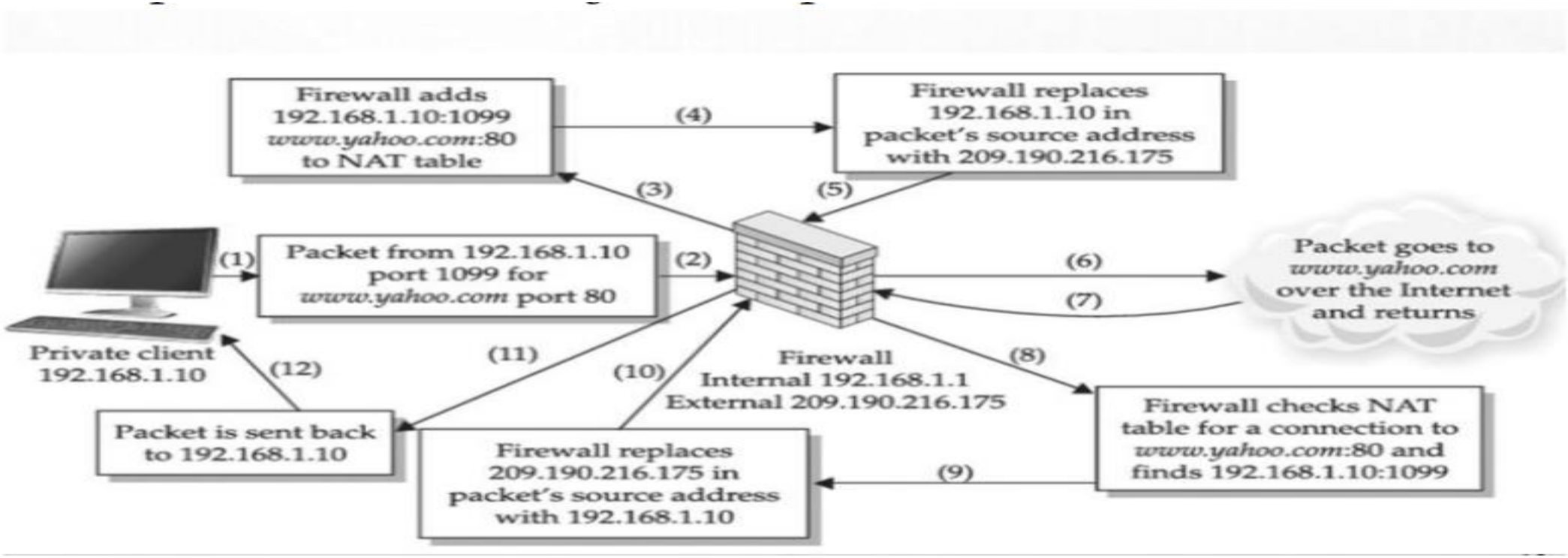
NAT CONT…

- IPv4 supports about 4 billion devices theoretically due to its 32-bit address field, and IPv6 uses a 128-bit address field, enough for roughly 3.4 × 1038 unique devices.
- The "non-routable" nature of private address spaces poses a problem once a device needs to access the Internet. Network Address Translation (NAT) solves this routing problem by translating packets from private to public addresses.
- NAT is usually performed by a networking device on its external interface for the benefit of the systems on its internal interface.
- Private systems can communicate with the Internet using the routable, publicly accessible IP address on the NAT device's external interface.
- When a NAT device receives traffic from the private network destined for the external network (Internet), it records the packet's source and destination details. The device then rewrites the packet's header such that the private source IP address is replaced with the device's external, public IP address.

NAT CONT…

- Then the device sends the packet to the destination IP address. From the destination system's point of view, the packet appears to have come directly from the NAT device. The destination system responds as necessary to the packet, sending it back to the NAT device's IP address.
- When the NAT device receives the response packet, it checks its address translation table to see if the address and port information of the packet match any of the packets that had been sent out.
- If no match is found, the packet is dropped or handled according to any firewall rules operating on the device. If a match is found, the NAT device rewrites the packet's destination IP address with the private IP address of the system that originally sent the packet.
- Finally, the NAT device sends the packet to its internal destination. The network address translation is completely transparent to the systems on the internal, private IP address and the Internet destination. The private system can access the Internet, but an Internet system cannot directly address it.

NAT CONT...


Firewall adds
192.168.1.10:1099
www.yahoo.com:80
to NAT table
(4)
Firewall replaces
192.168.1.10 in
packet's source address
with 209.190.216.175
(3)
(5)
(1)
Packet from 192.168.1.10
port 1099 for
www.yahoo.com port 80
(2)
(6)
(7)
Packet goes to
www.yahoo.com
over the Internet
and returns
Private client
192.168.1.10
(12)
(11)
(10)
Firewall
Internal 192.168.1.1
External 209.190.216.175
(8)
Packet is sent back
to 192.168.1.10
Firewall replaces
209.190.216.175 in
packet's source address
with 192.168.1.10
(9)
Firewall checks NAT
table for a connection to
www.yahoo.com:80 and
finds 192.168.1.10:1099

NAT CONT…

- NAT has a few limitations with regard to the kinds of traffic it may successfully translate.
- NAT has become integral to firewalls and network security. It provides an added layer of security to a firewall appliance, as it not only protects machines behind its internal interface, but also hides them.
- If we decide we'd like to expose a particular service on our private network to the Internet ,then we can use a technique called Port forwarding
- The NAT device may forward traffic received on a particular port on the device's external interface to a port on a system on the private, internal network. A remote system on the Internet that connects to the NAT device on this port effectively connects to the port on the internal system and only needs to know the public IP address of the NAT device.
- Now we've made our private network a little less private by exposing the service listening on that port. Now anyone on the Internet can access our internal web server by connecting to the port on our NAT device.
- If our NAT device is a firewall, we can use firewall rules to limit which IP addresses are allowed to access it.

THANK YOU