# Introduction to Firewall

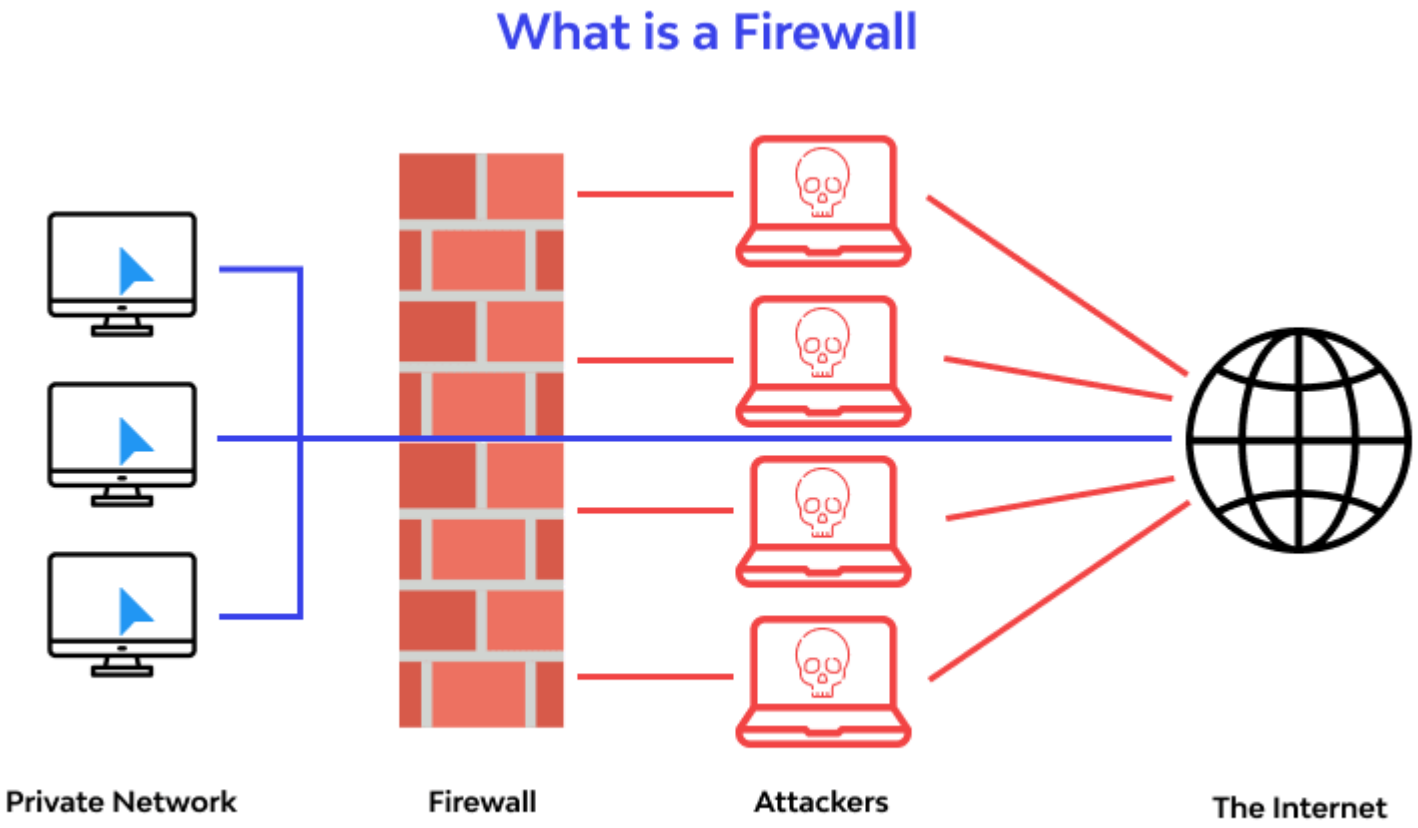
# Learning Objectives

**At the end of this learning activity, you should be able to:**

1. Articulate computer and network firewalls and their basic operations
2. Articulate static packet filtering and its usefulness
3. Articulate the basic operations of a stateful packet connection
4. Articulate the basic operations of NAT
5. Articulate application proxy firewalls and list the details of content filtering using firewalls

# Firewall

## What is a Firewall



# Firewall

**What is a Firewall?**

- It acts as a barrier between trusted and untrusted networks.
- It monitors and controls network traffic based on predetermined security rules.
- Filters incoming and outgoing traffic
- Prevents unauthorized access.
- *Example*: When you access an online banking website from your home, your home router's firewall helps ensure unauthorized parties can't easily access your network.

# Types of Firewall

I. Firewall Types by Systems Protected
II. Firewall Types by Form Factor
III. Firewall Types by Network Placement
IV. Firewall Types by Data Filtering Method

# Firewall Types by Systems Protected

- Network Firewall
- Host-Based Firewall

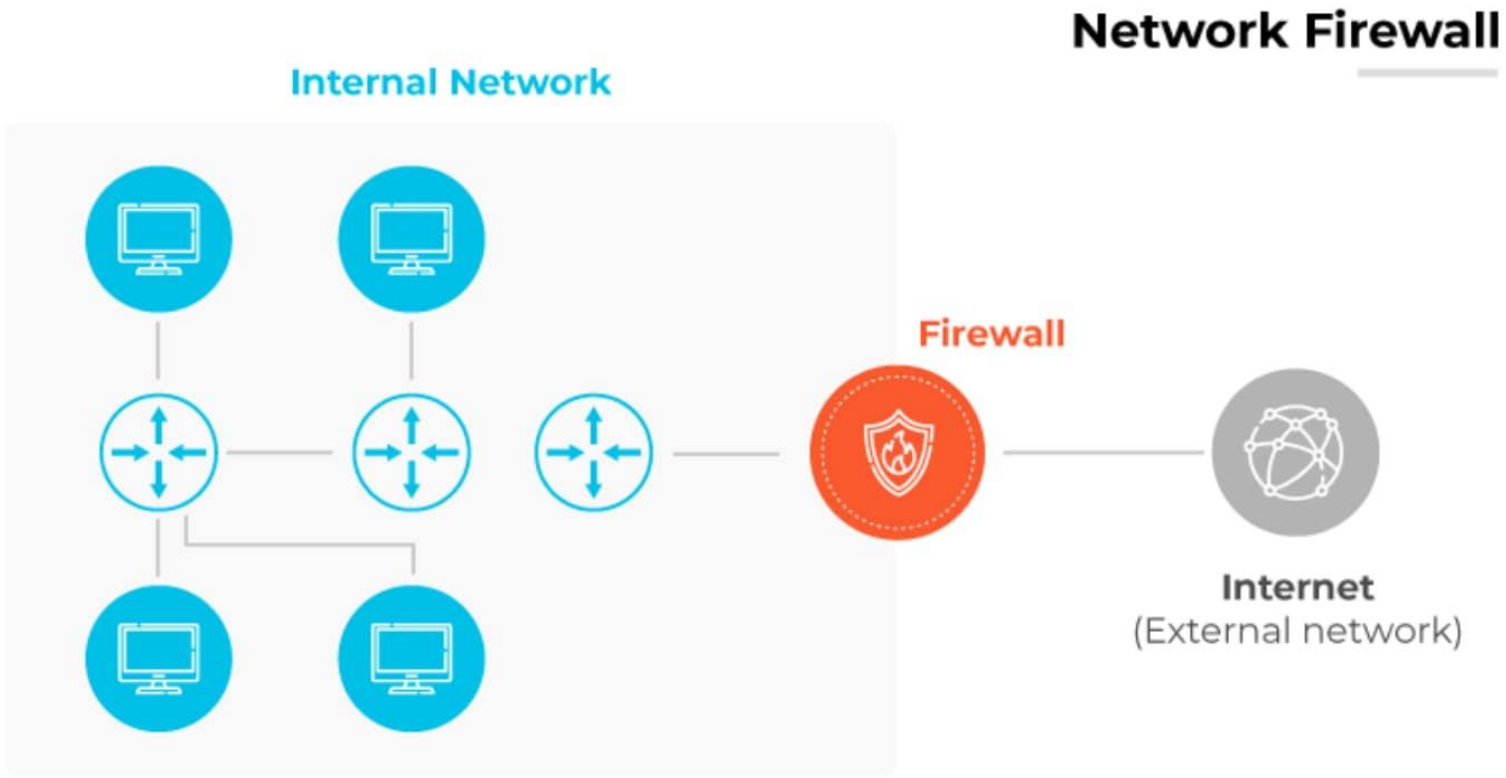
## I. Firewall Types by Systems Protected

### 1) Network Firewall

- positioned at the *juncture* between trusted and untrusted networks, such as internal systems and the internet.
- Its primary role is to monitor, control, and decide on the validity of incoming and outgoing traffic based on a predefined set of **rules**.
- These rules are designed to prevent unauthorized access and maintain network integrity.
- It effectively blocks potential threats or undesired data flow by *comparing* packet attributes like *source* and *destination IP addresses*, *protocol*, and *port numbers* to its **established rules**.

# I. Firewall Types by Systems Protected

## 1) Network Firewall



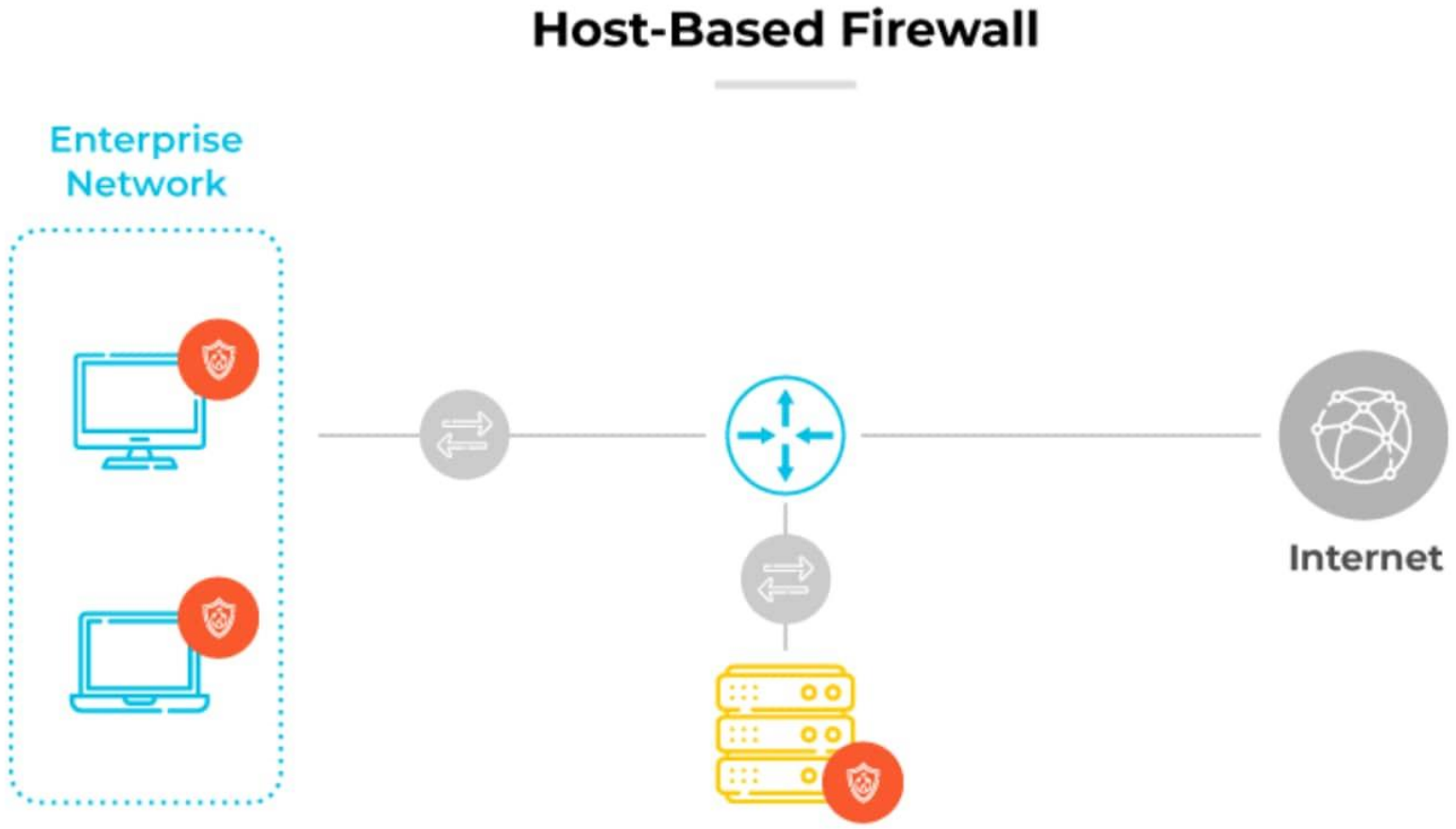
## I. Firewall Types by Systems Protected

### 2) Host-Based Firewall

- It is software that operates on a *single device* within a network.
- It is installed directly onto *individual computers* or *devices*, offering a focused layer of protection against potential threats.
- It effectively filters harmful content by examining that specific device's incoming and outgoing traffic, ensuring that malware, viruses, and other malicious activities do not infiltrate the system.

# I. Firewall Types by Systems Protected

## 2) Host-Based Firewall



# Firewall Types by Form Factor

- Hardware Firewall
- Software Firewall

## II. Firewall Types by Form Factors

### 1) Hardware Firewall

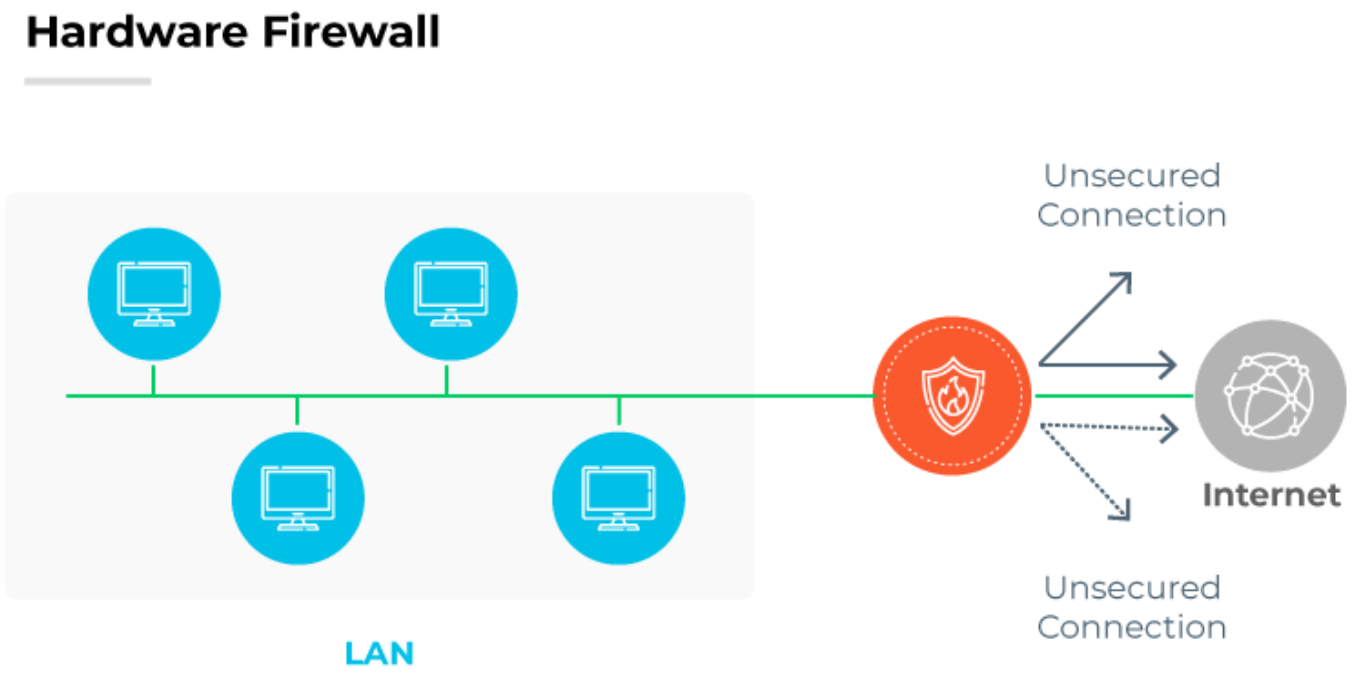
- It is a physical device placed between a computer or network and its connection to the Internet.
- It operates independently of the host device, examining inbound and outbound traffic to ensure compliance with set security rules.
- The hardware firewall can identify and block threats by actively analyzing data packets, providing a robust barrier against potential cyber intrusions.
- Once implemented, all internet traffic, whether incoming or outgoing, must pass through this device.

1U Rackmount Firewall Hardware with VPN, Network Security Appliance, Intel Atom N2600, 4 x Intel...

Visit ›

# II. Firewall Types by Form Factors

## 1) Hardware Firewall



## II. Firewall Types by Form Factors

### 2) Software Firewall

- It is a firewall in a software form factor rather than a physical appliance, which can be deployed on servers or virtual machines to secure cloud environments.
- They are designed to protect sensitive data, workloads, and applications in environments where it is difficult or impossible to deploy physical firewalls.
- Software firewalls embody the same firewall technology as hardware firewalls (also known as next-generation firewalls or NGFWs).
- They offer multiple deployment options to match the needs of hybrid/multi-cloud environments and modern cloud applications. Software firewalls can be deployed in any virtualized network or cloud environment.

# II. Firewall Types by Form Factors

**Types of Software Firewalls**

a) Container Firewalls
b) Virtual Firewalls
c) Cloud Firewalls
d) Managed Service Firewalls

# II. Firewall Types by Form Factors

## Types of Software Firewalls

### a) Container Firewalls

- A container firewall is a software version of a next-generation firewall that is purpose-built for *Kubernetes* environments.
- Container workloads embedded in Kubernetes environments can be complex and difficult to secure with traditional firewalls.
- container firewalls help network security teams safeguard developers with deep security integration into Kubernetes orchestration, preventing modern application attacks and data exfiltration.

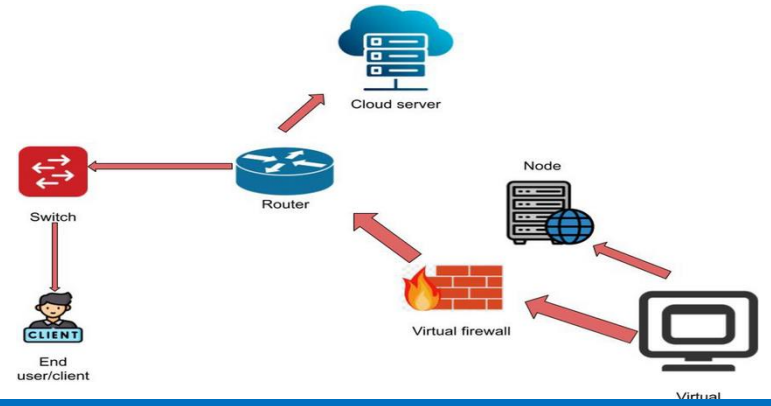
# II. Firewall Types by Form Factors

## Types of Software Firewalls

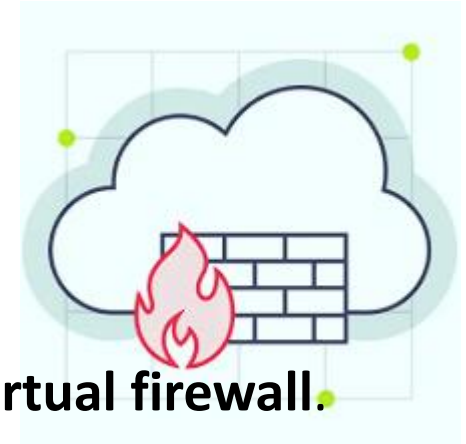
### b) Virtual Firewalls

- IT is a virtualized instance of a next-generation firewall, used in virtual and cloud environments to secure east-west and north-south traffic. They are sometimes referred to as "***cloud firewalls***."
- It is a software firewall that inspects and controls north-south perimeter network traffic in public cloud environments and segments east-west traffic inside physical data centers and branches.

- Virtual firewalls offer advanced threat prevention measures via micro-segmentation.



# II. Firewall Types by Form Factors



## Types of Software Firewalls

### c) Cloud Firewalls

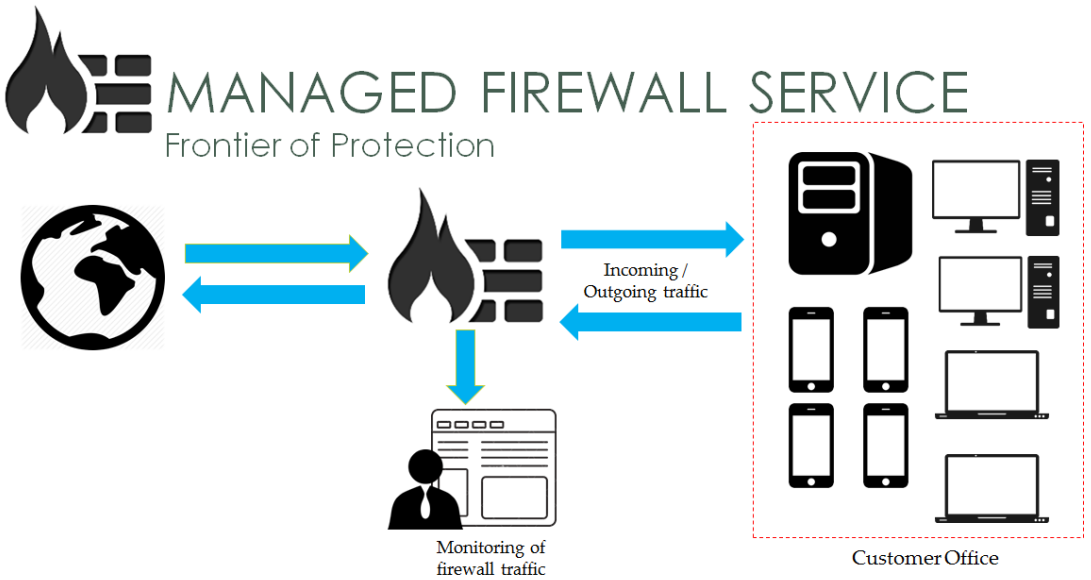
- The term “cloud firewall” aligns most closely with the concept of a **virtual firewall.**
- These are software-based mechanisms anchored in the cloud, primarily responsible for sifting out malevolent network traffic.
- The delivery model in the cloud has led to common identification as f**irewall-as-a-service** (FWaaS).
- A noteworthy iteration of this terminology is the "public cloud firewall." Emphasizing public cloud deployment, this concept fundamentally mirrors hardware firewalls in function.
- Predominantly, the term refers to firewalls situated in the cloud and offered by **security providers**, capabilities directly furnished by cloud hyperscalers, or appliances guarding applications within assorted public clouds

# II. Firewall Types by Form Factors

## Types of Software Firewalls

### d) Managed Service Firewalls

- Software firewalls are also available as a managed service, similar to many other **software-as-a-service (SaaS)** offerings.
- Some managed service firewall offerings provide a flexible way to deploy **application-level (Layer 7)** security without the need for management oversight.
- As managed services, some of these firewalls can be quickly scaled up and down



# Firewall Types by Placement within the Network Infrastructure

- Internal Firewall
- Distributed Firewall
- Perimeter Firewall

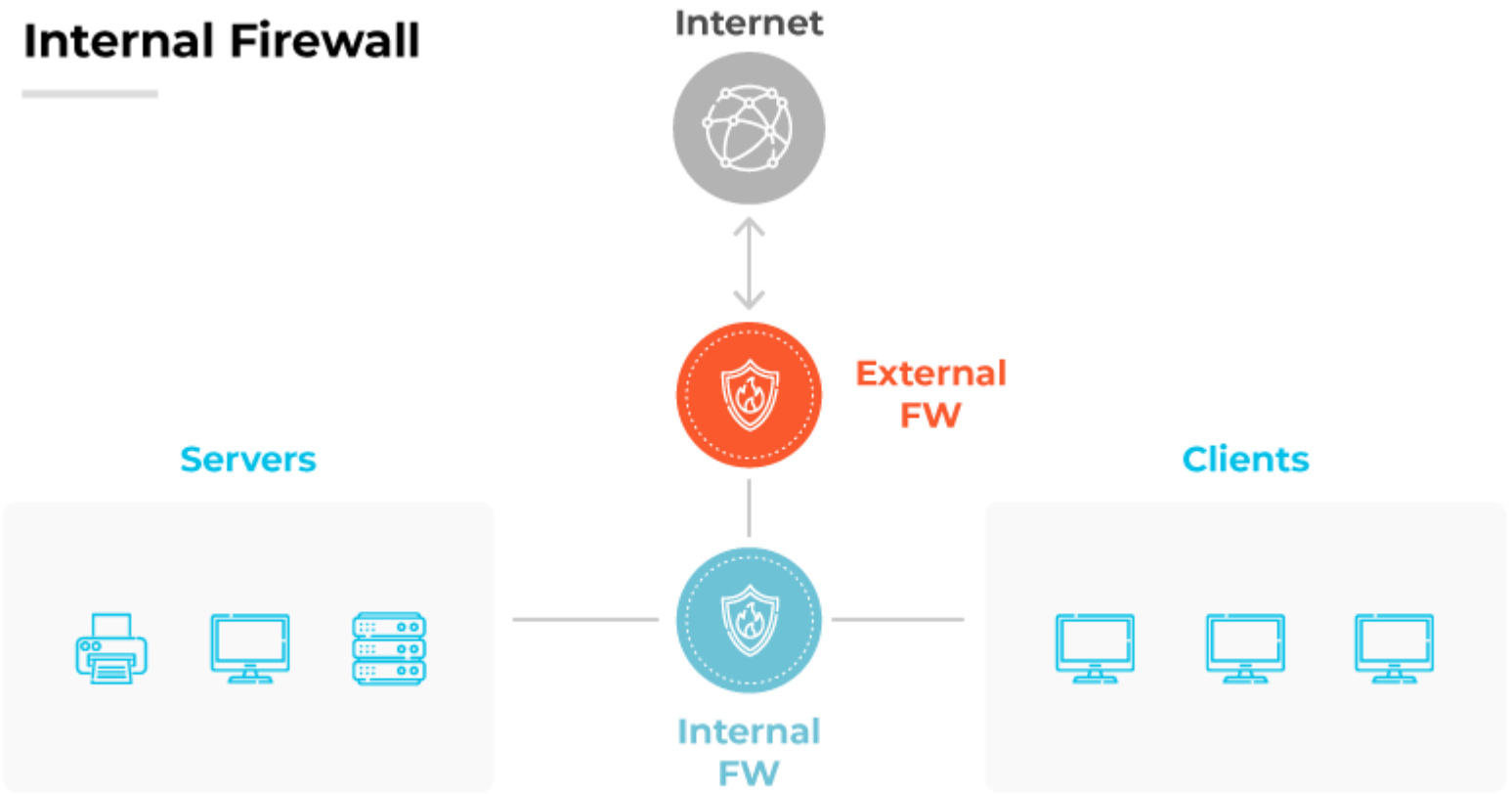
# III. Firewall Types by Network Placement

## 1) Internal Firewall

- An internal firewall functions primarily **within a network's confines**, targeting security threats that may have already penetrated the perimeter defenses.
- Unlike external or perimeter firewalls, which focus on incoming external threats, internal firewalls concentrate on the traffic between devices within the network.
- This is relevant because not all threats originate from the internet. Issues can arise within an organization, including unintentional *employee errors* or *malicious intentions*.
- This type of firewall operates under the principle of **Zero Trust**. It doesn't automatically trust any activity just because it originates from within the network.

# III. Firewall Types by Network Placement

## 1) Internal Firewall



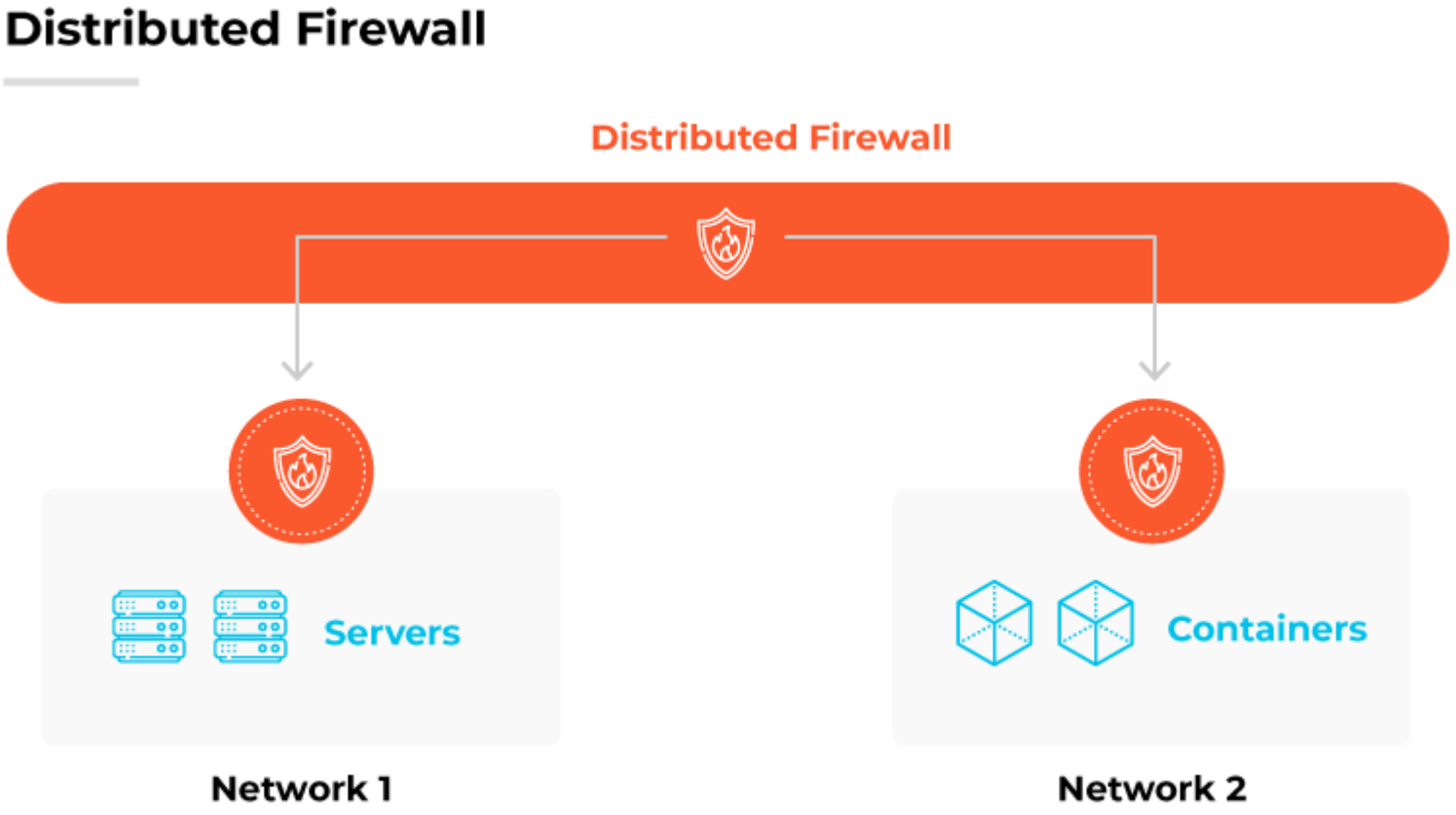
# III. Firewall Types by Network Placement

## 2) Distributed Firewall

- A distributed firewall is a network security mechanism that safeguards an organization's infrastructure.
- Unlike traditional firewalls, which are typically concentrated on a single node or device, distributed firewalls operate across a network.
- They harness the capabilities of multiple devices to monitor and regulate traffic, ensuring consistent and complete protection.
- It can monitor both internal and external traffic, examining traffic both within and entering the network, thus offering a more comprehensive security layer.
- It decentralizes the traffic monitoring process across numerous devices or nodes, preventing bottlenecks and points of congestion.

# III. Firewall Types by Network Placement

## 2) Distributed Firewall



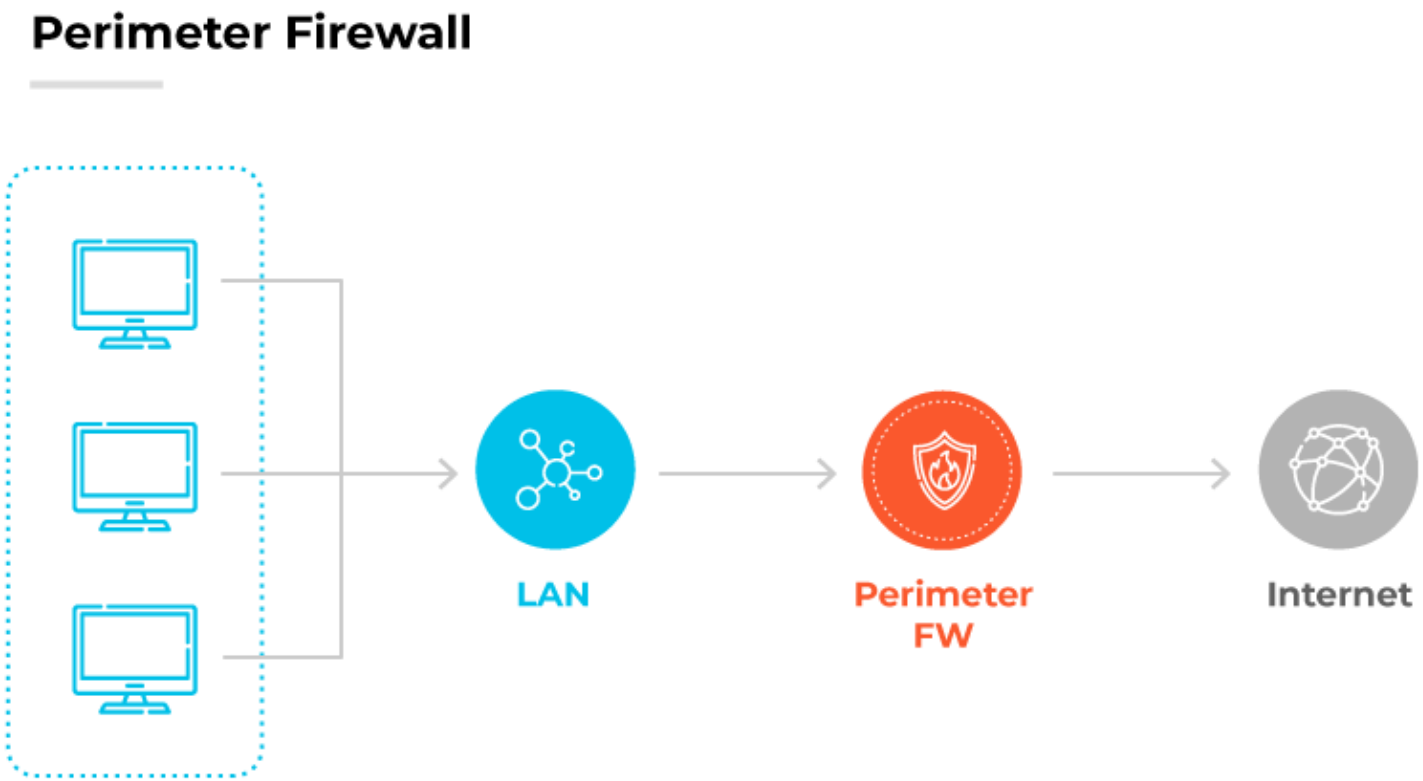
# III. Firewall Types by Network Placement

## 3) Perimeter Firewall

- A perimeter firewall establishes the boundary between a private network and the public domain of the Internet.
- As the primary defense, this firewall meticulously inspects every data byte attempting to pass through.
- This safeguards the private network from unwarranted and potentially harmful data.
- A significant role of a perimeter firewall involves differentiating and subsequently allowing or disallowing traffic based on pre-defined parameters, ensuring only legitimate and safe data gains entry.
- The efficacy of a perimeter firewall hinges on its ability to recognize and discern the nature of data packets.
- It examines both the header information and the payload of each packet to determine intent.

# III. Firewall Types by Network Placement

## 3) Perimeter Firewall



# III. Firewall Types by Network Placement

## 3) Perimeter Firewall

- A perimeter firewall establishes the boundary between a private network and the public domain of the Internet.
- As the primary defense, this firewall meticulously inspects every data byte attempting to pass through.
- This safeguards the private network from unwarranted and potentially harmful data.
- A significant role of a perimeter firewall involves differentiating and subsequently allowing or disallowing traffic based on pre-defined parameters, ensuring only legitimate and safe data gains entry.
- The efficacy of a perimeter firewall hinges on its ability to recognize and discern the nature of data packets.
- It examines both the header information and the payload of each packet to determine intent.

# Firewall Types by Data Filtering Method

- Internal Firewall
- Distributed Firewall
- Perimeter Firewall

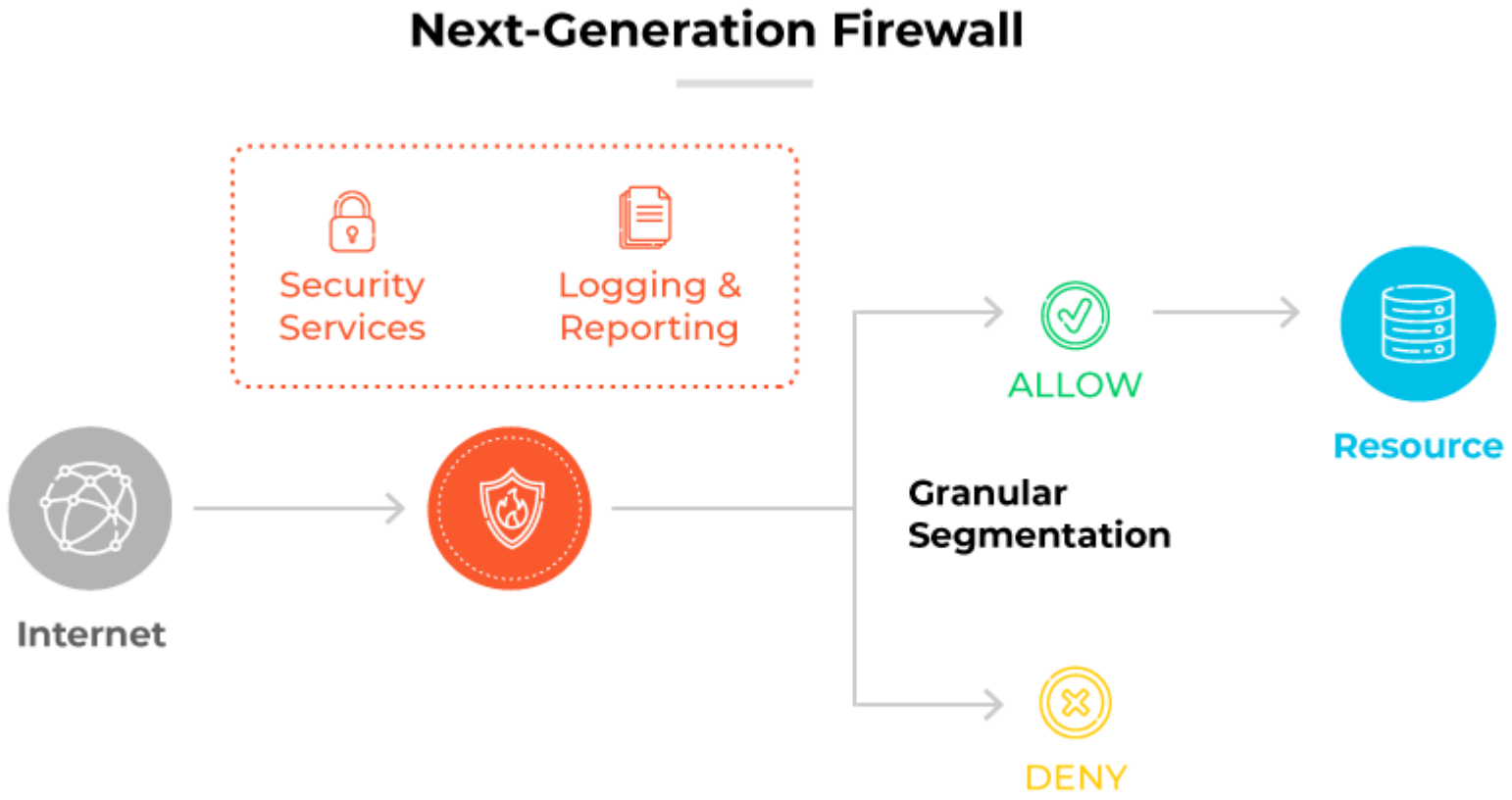
# IV. Firewall Types by Data Filtering Method

## 1) Next-generation Firewall

- A next-generation firewall (NGFW) extends the capabilities of traditional firewalls, offering more comprehensive security solutions.
- Unlike their predecessors focused primarily on stateful inspection, NGFWs provide enhanced features to understand and control application traffic, integrate intrusion prevention mechanisms, and utilize cloud-sourced threat intelligence.
- This evolved approach ensures a more meticulous inspection of data packets, accounting for the intricate nuances of modern cyber threats.
- The integration of threat intelligence sources within NGFWs ensures they remain updated with the latest threat vectors, maintaining their effectiveness against evolving cybersecurity challenges.

# IV. Firewall Types by Data Filtering Method

## 1) Next-generation Firewall



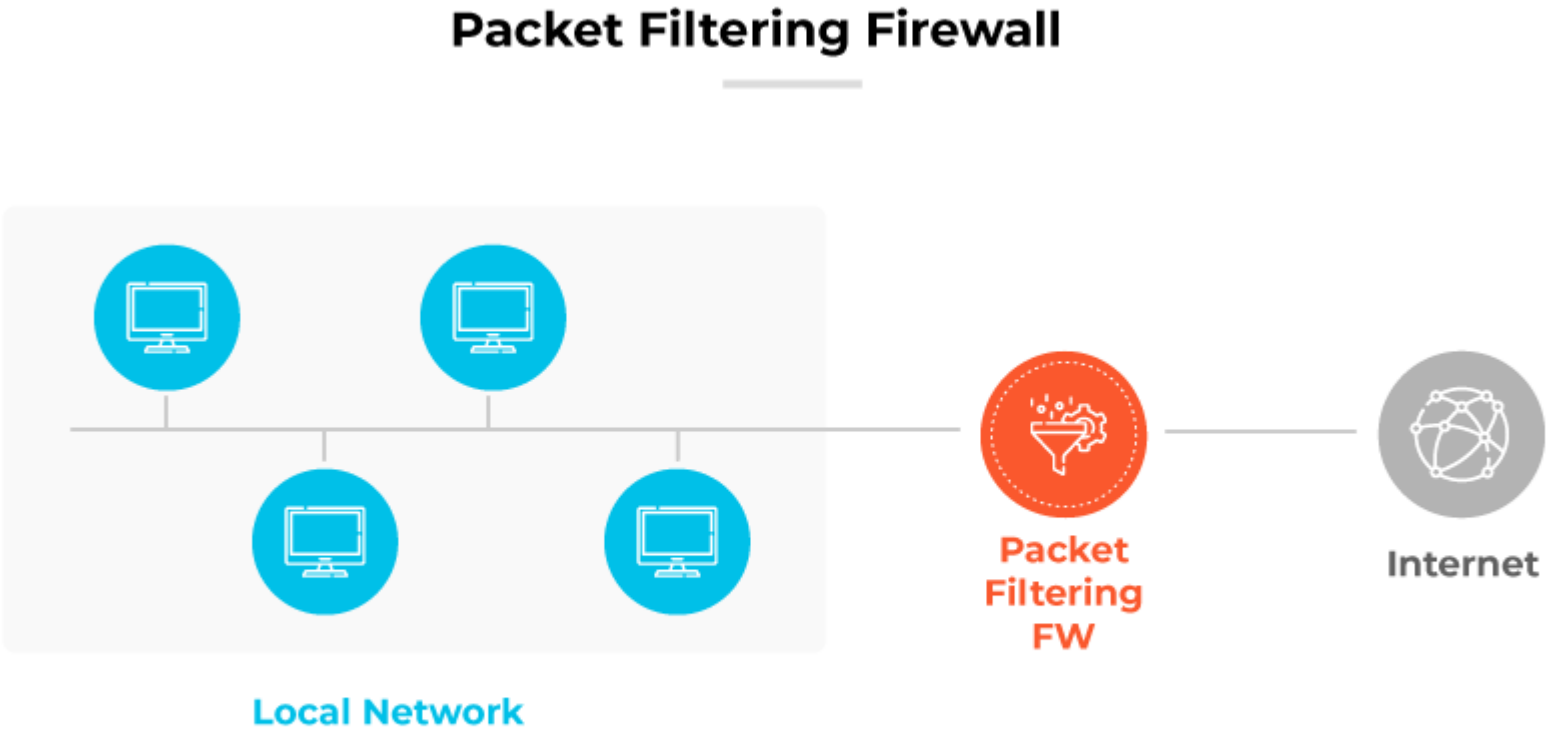
# IV. Firewall Types by Data Filtering Method

## 2) Packet Filtering Firewall

- Packet filtering firewalls operate at the *network layer*, regulating data packet flow between networks.
- These firewalls rely on pre-defined rules that evaluate specific attributes of the packets, such as source *IP, destination IP, ports*, and *protocols*.
- If the attributes match the established rules, the packet is allowed to pass through. If not, the packet is blocked.
- Types of packet filtering firewalls can be further broken down into *static packet-filtering firewalls*, *dynamic packet-filtering firewalls*, *stateless packet-filtering firewalls*, *stateful packet-filtering firewalls*.

# IV. Firewall Types by Data Filtering Method

## 2) Packet Filtering Firewall



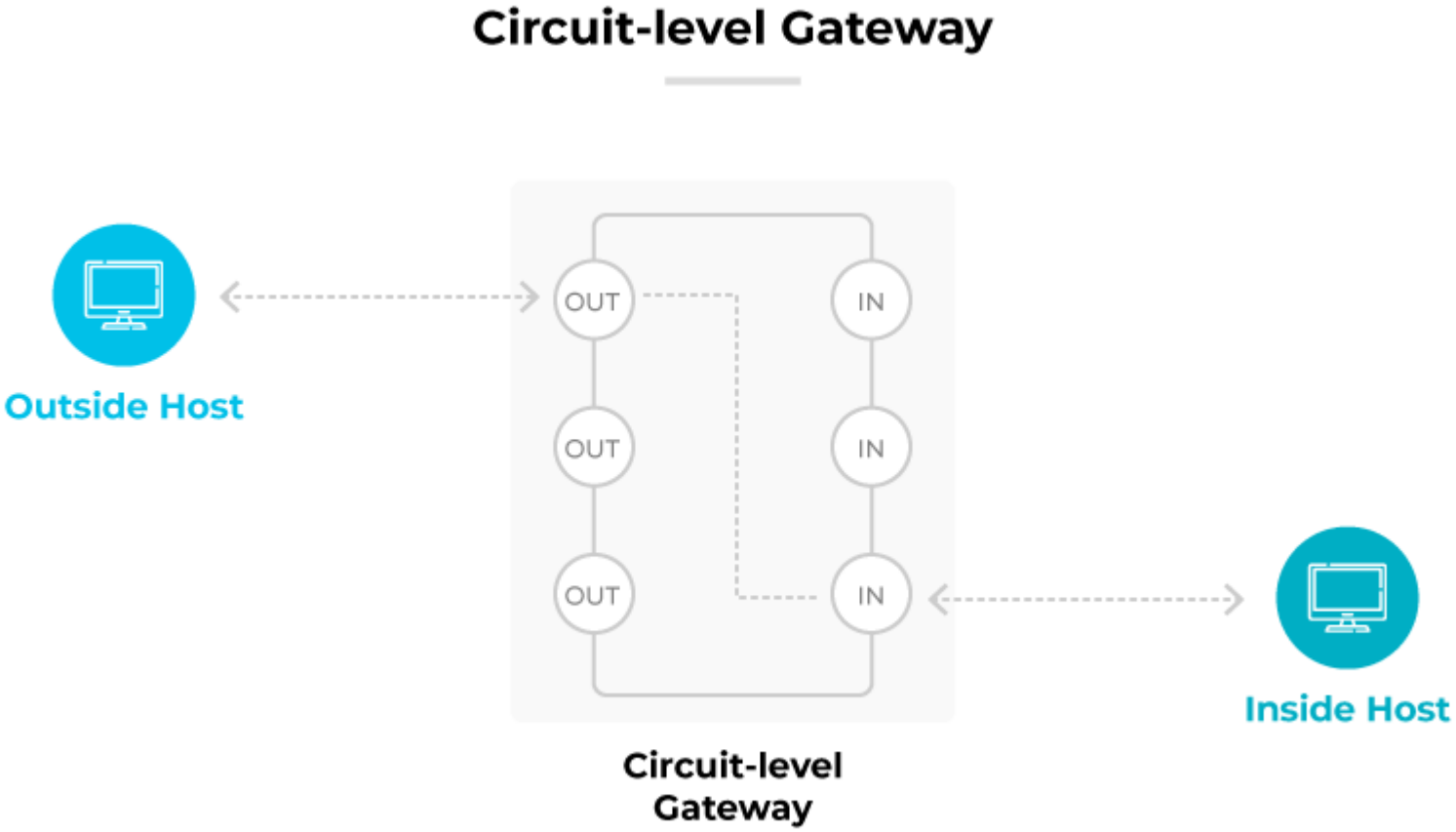
# IV. Firewall Types by Data Filtering Method

## 3) Circuit Level Gateway

- A circuit-level gateway functions primarily at the *session layer* of the OSI model.
- It oversees and validates the *handshaking* process between packets, specifically for **TCP** and **UDP** connections.
- By examining the handshake process and the IP addresses associated with packets, this firewall identifies legitimate traffic and deters unauthorized access.
- A circuit-level gateway primarily focuses on *header information*, ensuring the traffic aligns with the firewall's rule set without delving into the actual content of the data packets.

# IV. Firewall Types by Data Filtering Method

## 3) Circuit Level Gateway



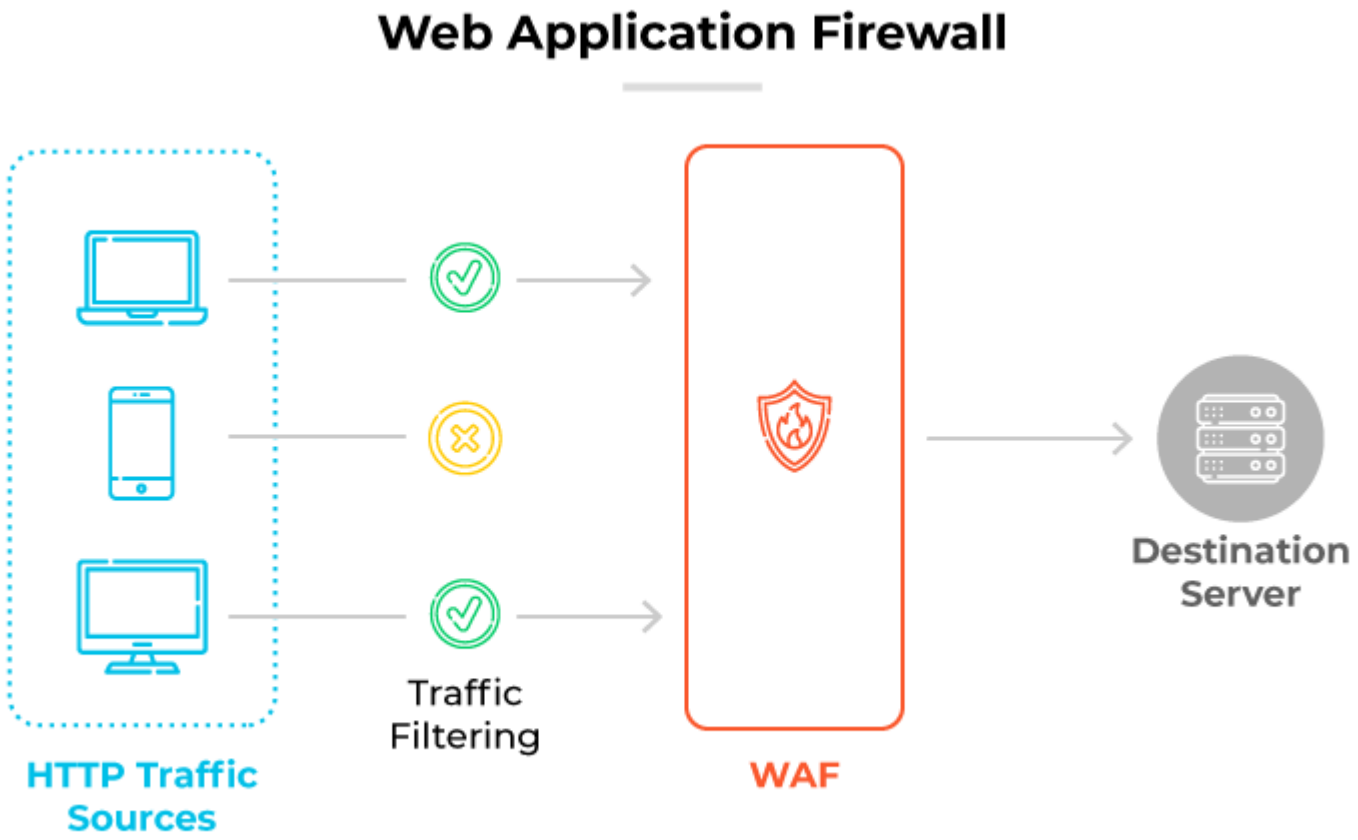
# IV. Firewall Types by Data Filtering Method

## 4) Web Application Firewall

- A web application firewall, commonly called *WAF*, serves as a specialized layer of protection for web applications, web servers, and APIs.
- It examines and filters *HTTP traffic* by safeguarding web applications from threats like cross-site-scripting (XSS), SQL injection, and file inclusion.
- WAFs differentiate themselves by operating at *Layer 7*, specifically targeting application layer threats.
- Positioned in front of web applications, WAFs act as reverse proxies.
- This means that they intercept and inspect requests bound for the web application, ensuring only legitimate traffic passes through

# IV. Firewall Types by Data Filtering Method

## 4) Web Application Firewall



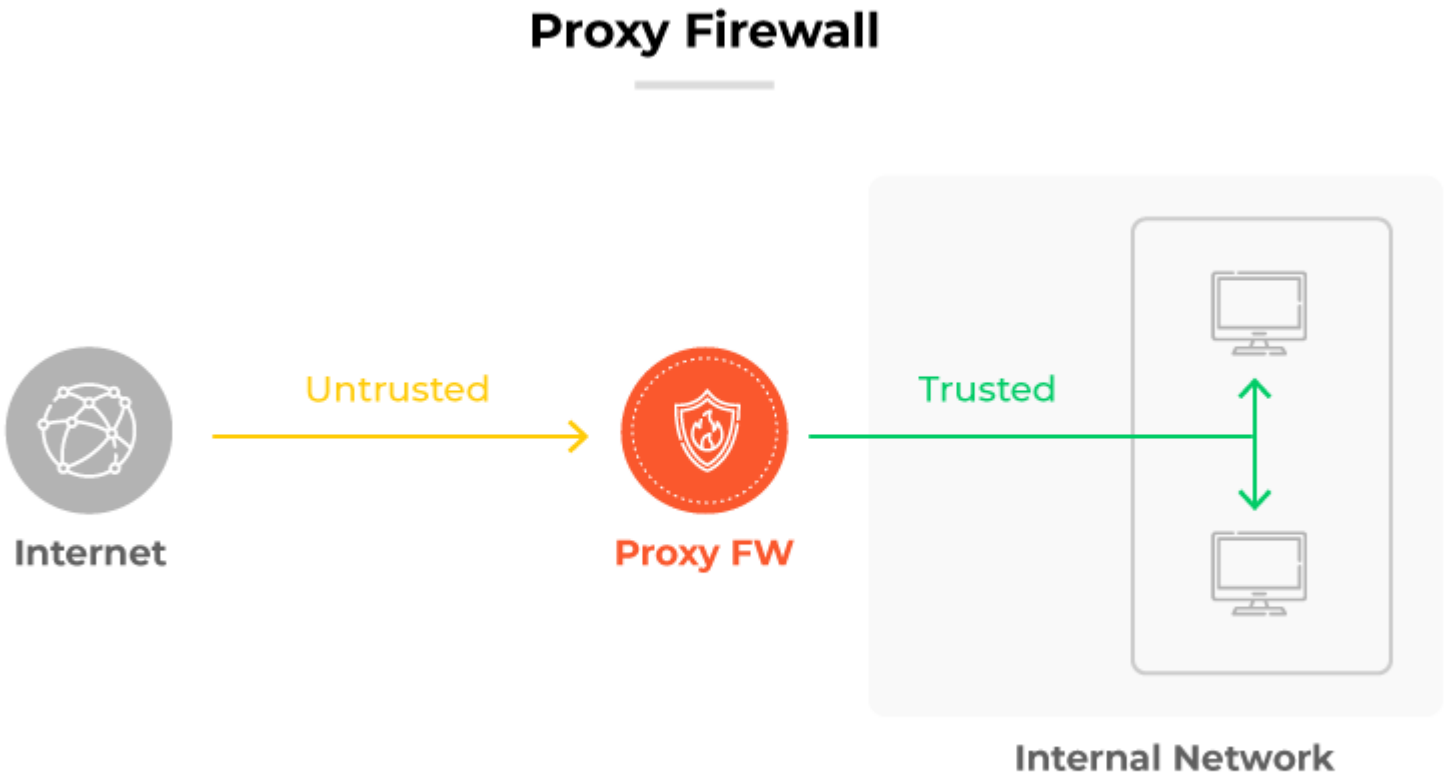
# IV. Firewall Types by Data Filtering Method

## 4) Proxy Firewall

- A proxy firewall is a vital network defense mechanism, operating at the *application layer*.
- Also referred to as an *application firewall* or *gateway firewall*, it primarily functions as an intermediary, filtering messages between computer systems and external servers.
- Computers within a network connect to the Internet using a proxy as their gateway. When a user attempts to access an external website or service, their request is intercepted by the proxy firewall.
- This firewall evaluates the request against its set policies, if deemed safe, it establishes a connection on behalf of the user.

# IV. Firewall Types by Data Filtering Method

## 4) Proxy Firewall



# IV. Firewall Types by Data Filtering Method

## 5) Stateful Inspection Firewall

- Stateful inspection firewalls are integral in active network connection monitoring.
- By tracking these connections, they analyze the context of incoming and outgoing traffic, ensuring only safe data packets traverse the network.
- Located at *Layers 3 and 4* of the Open Systems Interconnection (OSI) model, their primary function is to filter traffic based on its state and context.
- This method is more thorough than packet-level protection because it understands the broader context of data exchanges.
- It scrutinizes the contents of each data packet to determine if it matches the attributes of previously recognized safe connections.

# IV. Firewall Types by Data Filtering Method

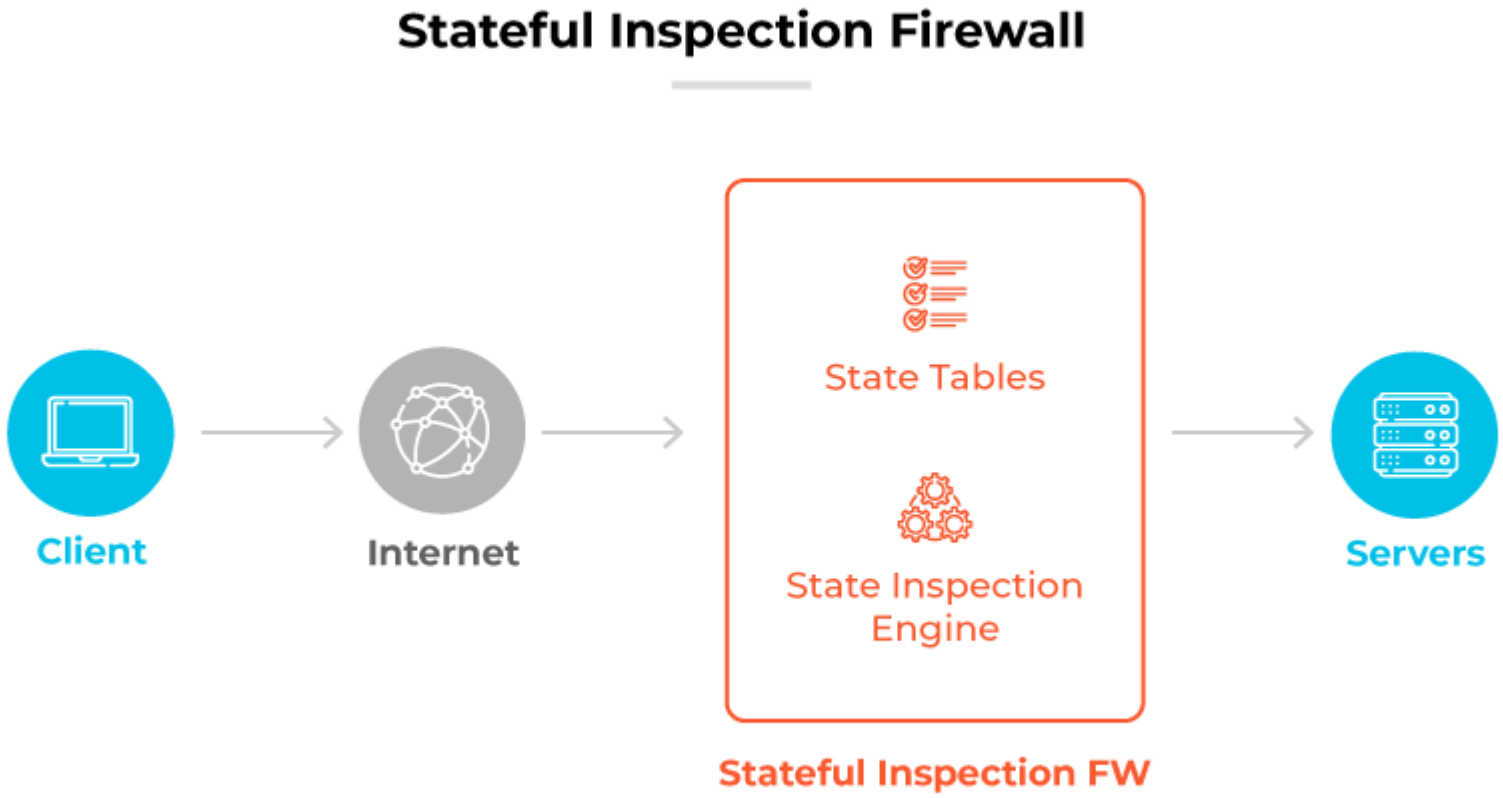
## 5) Stateful Inspection Firewall

*Example*:

- TCP facilitates the simultaneous sending and receiving of data and uses a three-way handshake process to establish connections.
- The handshake involves synchronization (SYN), synchronization-acknowledge (SYN-ACK), and acknowledgment (ACK).
- The stateful firewall utilizes this process to recognize potential threats by examining packet contents during the handshake. If any red flags arise, such as suspicious origins or destinations, the firewall immediately discards the data. This approach ensures that only legitimate and secure connections are maintained.

# IV. Firewall Types by Data Filtering Method

## 5) Stateful Inspection Firewall



# Network Address Translation (NAT)

- How NAT Works
- Examples of NAT
- Types of NAT

# Network Address Translation

## Network Address Translation (NAT)

- **Network Address Translation (NAT)** is a method used in networking where private (internal) IP addresses are translated into a public IP address before packets are forwarded to the external network (typically, the internet).
- It **hides** the internal network structure from the outside world and **conserves public IP addresses**.

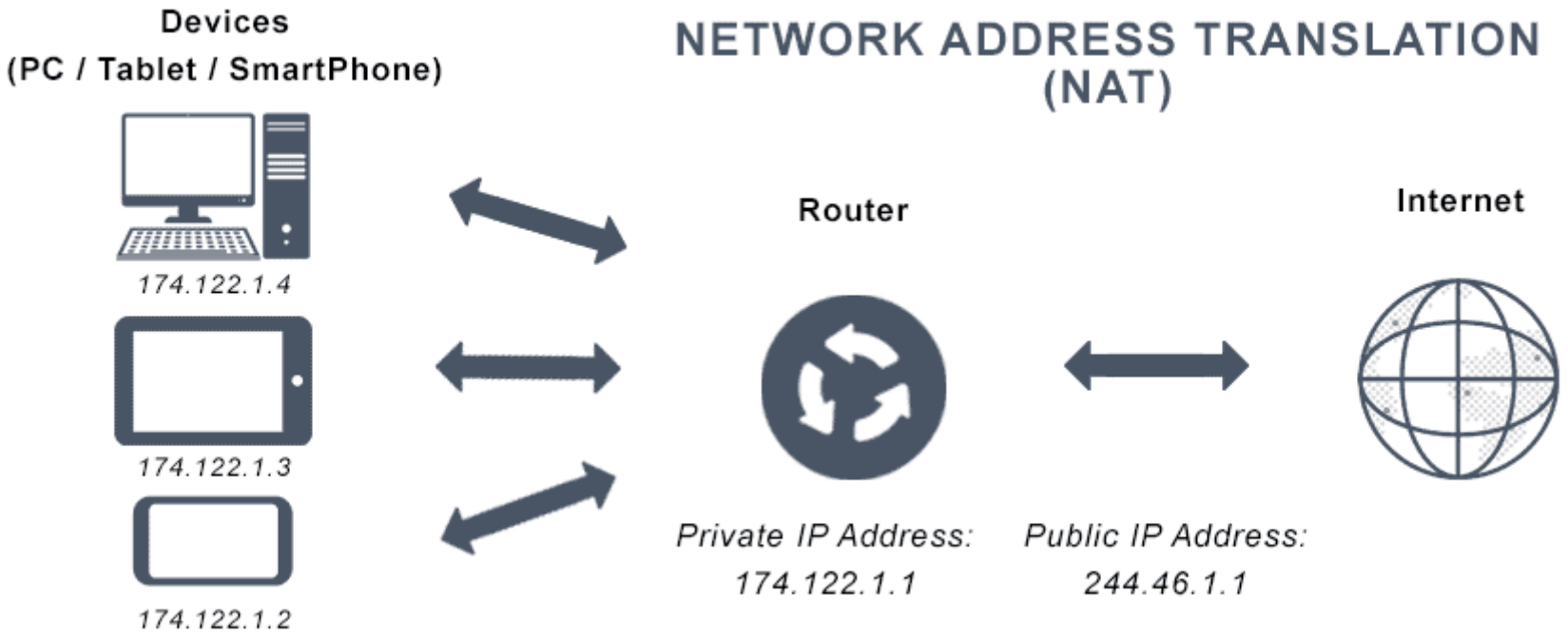
# Network Address Translation

## How NAT works

1. Devices in a local/private network are assigned private IP addresses (e.g., 192.168.x.x, 10.x.x.x).
2. When these devices access the internet, NAT translates their private IP addresses into a public IP address.
3. The router or firewall performing NAT keeps a translation table to track which private IP corresponds to which session on the public internet.
4. When responses from the internet come back, NAT rewrites the destination address back to the private IP and delivers it to the correct internal device.

# Network Address Translation

## Example of how NAT works



# Learning Activity

1. Define what a firewall is and explain its two main functions in a network.
2. Differentiate between a Packet-Filtering Firewall and a Stateful Inspection Firewall. Provide one advantage of a stateful firewall over a packet-filtering firewall.
3. Imagine you are setting up a firewall for a large enterprise. You want to protect internal confidential data, segment internal departments, and detect advanced threats like malware hidden in web traffic. Which type(s) of firewall would you deploy? Explain your choices in 2–3 sentences.
4. In your own words, explain how NAT enhances security for a private network. Give a specific example where NAT would be beneficial.

## Learning Activity

5. You are hired as a network security consultant for a university. The university needs to:
   - Allow students to browse the internet freely
   - Protect the university's internal databases
   - Block harmful or inappropriate websites

*Questions*:

a) What firewall configurations and placements would you recommend?

b) Sketch or describe your simple network security plan.