How Firewall Works

CYBER EDITION | NETWORK SECURITY | IT ADMINISTRATION

A comprehensive guide to network security for IT administrators and students — from basic principles to advanced filtering techniques, network segmentation, and Windows Server practice.

What Is a Firewall?

Definition

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a **security gateway** between your computer and the internet.

Three Core Actions

✓ Allow

Traffic meets security rules and may continue.

Block

Traffic is not permitted and is rejected or dropped.

⚙️ Inspect & Decide

Advanced firewall inspects content before deciding.

Types of Firewalls & Key Concepts

Hardware Firewall

A standalone physical device, often part of a router or enterprise security gateway. Used primarily in companies and data centers.

Software Firewall

A program running on a computer or server — e.g., **Windows Defender Firewall**. Suitable for individual users and servers alike.

Combined Firewall

A combination of hardware and software solutions. Provides the highest level of protection, used in critical enterprise environments.

Client

Device requesting access — PC, laptop, or phone. E.g., IPs: 10.10.10.4, 10.10.10.5, 10.10.10.6

Server

Provides a service to the client — web, database, email, or application server.

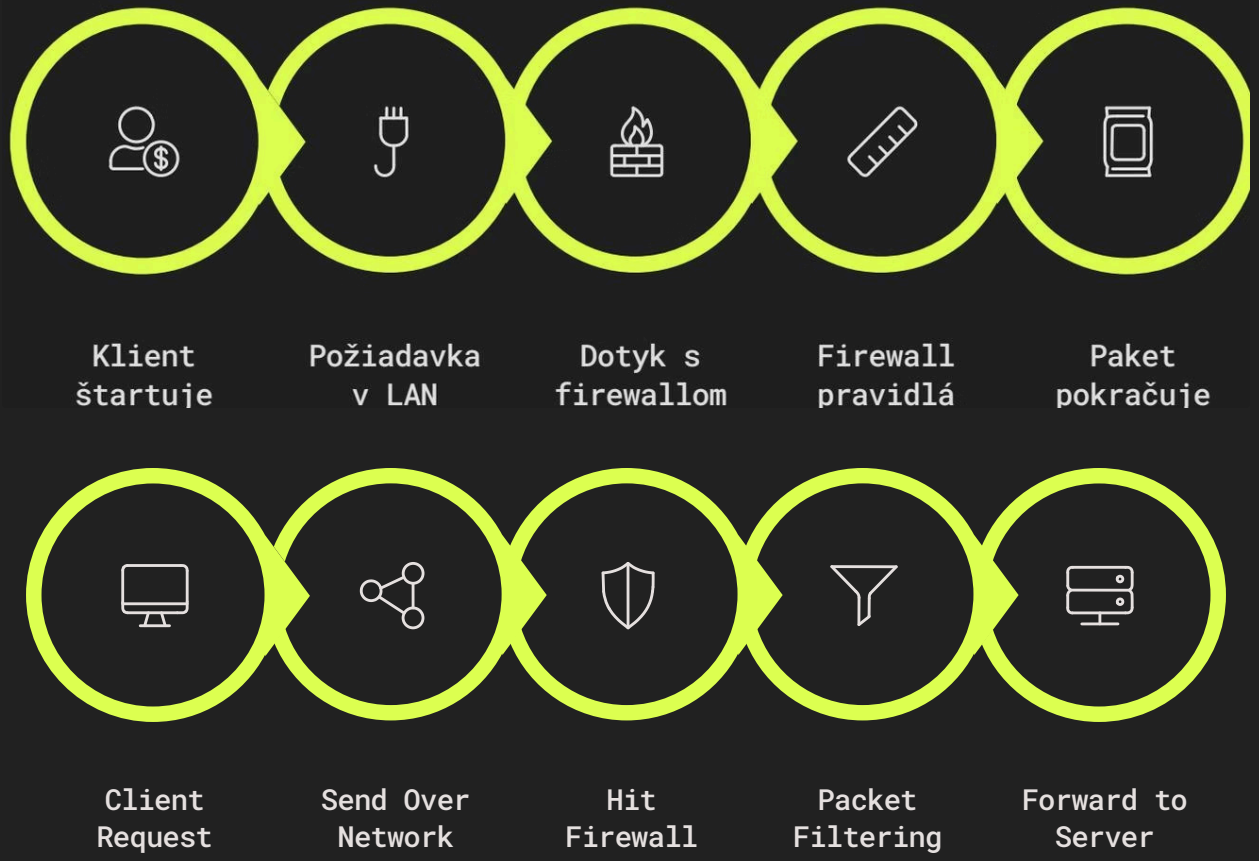
Router

Routes traffic between networks (LAN ↔️ Internet). Often includes firewall functions.

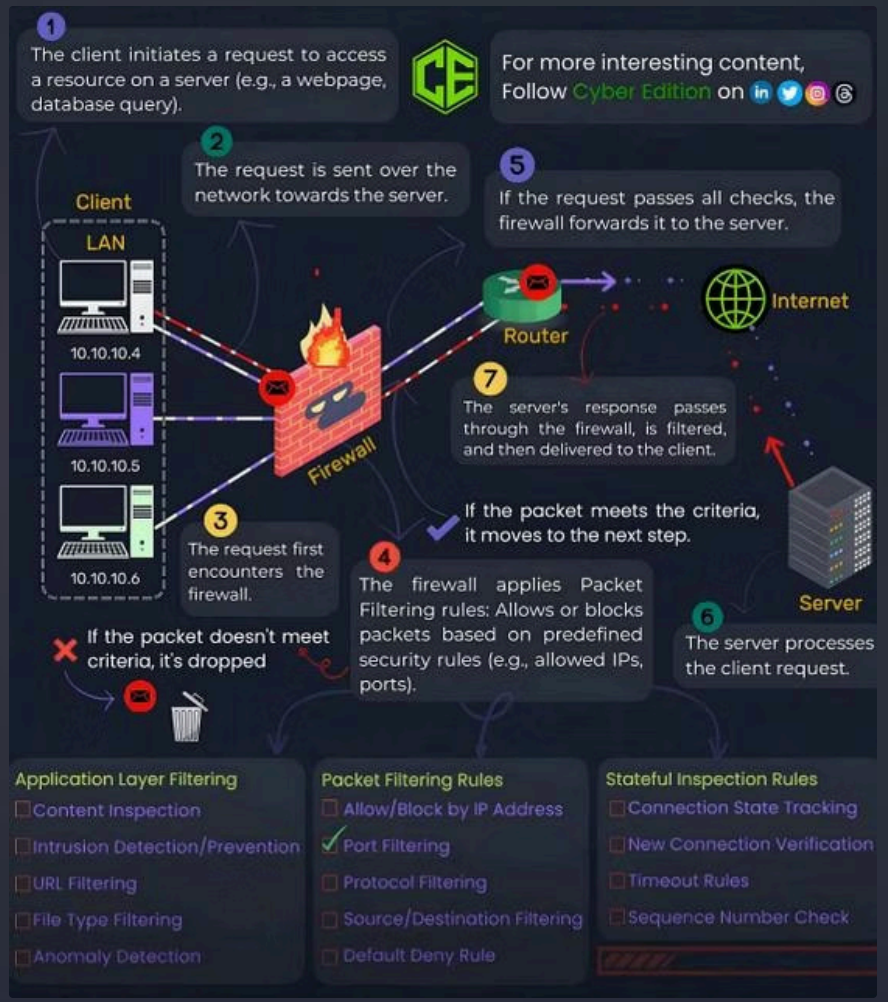
Packet

A small chunk of data containing source/destination IP, port, protocol, and payload.

How Firewall Works – Step by Step



Every packet passes through firewall rules **in both directions** — both the client request and the server response must meet security criteria. If a packet does not meet the rules, the firewall drops or blocks it.



Packet Filtering & Key Ports

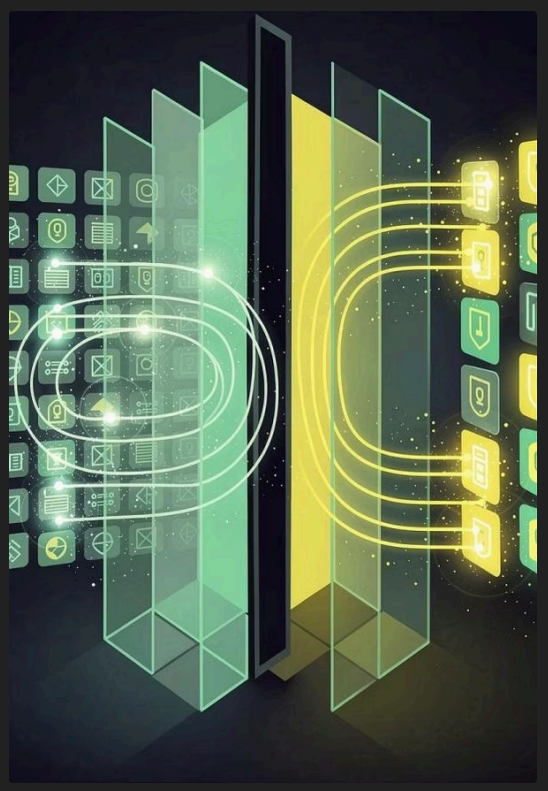
What the Firewall Checks

- Source IP address
- Destination IP address
- Port — source and destination
- Protocol — TCP, UDP, ICMP
- Direction — inbound / outbound

> ⚠ Default Deny Rule: Everything not explicitly permitted is blocked. This is the most important security principle.

Most Important Ports

Port	Service	Recommendation
80	HTTP	Prefer 443
443	HTTPS	Allow
22	SSH	Internal only
3389	RDP	**Never from internet!**
53	DNS	Allow TCP/UDP
445	SMB	LAN only
1433	MS SQL	App server only



Advanced Filtering Techniques

Stateful Inspection

Unlike basic packet filtering, stateful inspection **remembers the connection state** — it checks whether a packet belongs to an existing session.

State	Meaning
New	Unknown new connection
Established	Existing, permitted connection
Related	Related connection (e.g., FTP data)
Invalid	Invalid or suspicious connection

Unsolicited traffic from the internet without a prior request is **automatically blocked**. Timeout Rules terminate idle connections automatically.

Application Layer Filtering (NGFW)

Content Inspection

Checks for malicious code, dangerous files, and data leaks.

IDS / IPS

IDS detects attacks; IPS also **automatically blocks** them.

URL Filtering

Blocks phishing, malware, and unwanted website categories.

File Type Filtering

Blocks .exe, .bat, .ps1, .zip — reduces ransomware risk.

Anomaly Detection

Detects thousands of requests/sec, unusual country connections, or suspicious IPs.

Firewall in Practice — Enterprise Environment

Rule	Action	Reason
Employees → Internet TCP 443	✓ Allow	Encrypted web
Employees → DNS UDP/TCP 53	✓ Allow	Domain resolution
TCP 23 (Telnet)	✗ Block	Insecure protocol
RDP from Internet	✗ Block	High attack risk
DB ← App Server only	✓ Specific IP only	Access segmentation
Internet → LAN	✗ Block	Protect internal network
Everything else	✗ Default Deny	Security principle

ⓘ Best practice: Document every rule — include the reason, creation date, and responsible person.

Windows Defender Firewall — Domain Profiles

Domain

Computer is a domain member

Private

Trusted private network

Public

Public / untrusted network

Firewall Logs, SIEM & Troubleshooting

Why Firewall Logs Matter

Firewalls log every event — what was allowed or blocked, source, destination port, and timestamp. Logs are essential for:

- Security audit and compliance
- Investigating security incidents
- Detecting repeated attack attempts
- Integration with SIEM systems

Popular SIEM Tools

- Microsoft Sentinel
- Splunk
- QRadar (IBM)
- Elastic Security
- Wazuh (open-source)

⚠ Example: One IP attempts to connect to 500 different ports in 5 minutes → possible port scan → SIEM alerts the admin.

Troubleshooting Steps

"I cannot connect to an internal web application."

01

Check IP Address

`ipconfig` — identify client IP

02

Check Connectivity

`ping webserver01` — ICMP test

03

Check Port

`Test-NetConnection webserver01 -Port 443`

04

Review Rules

`Get-NetFirewallRule` — list rules

05

Check Logs

Event Viewer → Windows Defender Firewall logs

06

Fix the Rule

`New-NetFirewallRule -DisplayName "Allow HTTPS" -Direction Inbound -Protocol TCP -LocalPort 443 -Action Allow`

Network Segmentation & Zero Trust

Network Segmentation

A firewall can divide the network into isolated segments, reducing the risk of attack propagation.

Segment	Access
Guest Wi-Fi	Internet only, not LAN
Admin Network	Access to servers
Users	No DB access
App Server	DB access permitted
IoT Devices	Isolated network

Zero Trust Principle

Never trust automatically. Always verify.

Zero Trust assumes no communication — even internal — is automatically trusted.

Always Verify Identity

Least Privilege

Continuous Control

Common Configuration Mistakes

- Allow all — no protection
- RDP open to the internet — brute-force risk
- Missing Default Deny rule
- No logs — admin is blind
- No outbound traffic control — malware communicates freely

Summary — Key Takeaways

🔍 Controls Traffic

Allows or blocks packets by IP address, port, protocol, and direction.

🧠 Remembers State

Stateful inspection tracks existing connections and blocks unsolicited inbound traffic.

🔎 Inspects Content

Next-gen firewalls perform URL filtering, content inspection, IDS/IPS, and anomaly detection.

🌐 Part of an Ecosystem

Works with SIEM, VPN, Active Directory, network segmentation, and Zero Trust principles.

> A firewall doesn't decide by feeling — it decides by rules: **who** is communicating, **where** they're going, **which port**, **which protocol**, and whether that communication is **permitted**.

3

Firewall Types

Hardware, Software, Combined

7

Steps in Flow

Client to server and back

5

NGFW Features

Content, IDS/IPS, URL, File, Anomaly

0

Default Deny

Exceptions must be explicitly allowed