🔥 Was ist eine Firewall und wozu brauche ich sie?

📌 Grunddefinition

Eine **Firewall** (auf Deutsch: „Brandmauer“) ist eine **Sicherheitsvorrichtung**, die den **Datenverkehr zwischen Netzwerken überwacht und kontrolliert** – zum Beispiel zwischen dem Internet und deinem Heimnetzwerk oder zwischen verschiedenen Teilen eines Unternehmensnetzwerks.

Ziel einer Firewall:
➡️ **Unerlaubten Zugriff verhindern**
➡️ **Erlaubten Datenverkehr zulassen**

💡 Wofür steht der Begriff „Firewall“?

Der Begriff stammt ursprünglich aus dem **Brandschutz**: Eine „Feuerwand“ soll das **Übergreifen von Feuer**verhindern – genau wie die digitale Firewall das **Eindringen von Schadsoftware und Angreifern** verhindern soll.

🛡️ Was macht eine Firewall konkret?

Eine Firewall prüft alle Datenpakete, die **in dein Netzwerk hinein oder hinaus** wollen. Dabei entscheidet sie anhand von **Regeln**, ob ein Paket:

- **zugelassen (erlaubt)** oder
- **blockiert (verworfen)** wird.

Diese Regeln basieren z. B. auf:

- ✅ IP-Adressen
- ✅ Ports (z. B. Port 80 für Webseiten)
- ✅ Protokollen (z. B. TCP oder UDP)
- ✅ Zeitfenstern
- ✅ Anwendungen

🔍 Arten von Firewalls

🔷 1. Paketfilter-Firewall (Layer 3)

- Prüft Absender-IP, Ziel-IP, Portnummern
- Arbeitet schnell, aber oberflächlich
- Beispiel: Viele Router-Firewalls

🔷 2. Stateful Firewall

- Merkt sich, welche Verbindungen „erlaubt“ sind (Verbindungszustand)
- Blockiert unerwartete Antworten
- Standard in vielen modernen Netzwerken

🔷 3. Application Firewall

- Analysiert Anwendungen (z. B. erkennt sie Webbrowser oder E-Mail-Programme)
- Erlaubt sehr gezielte Kontrolle

🔷 4. Next Generation Firewall (NGFW)

- Kombiniert Paketfilter, Deep Packet Inspection, Virenschutz, VPN, IDS/IPS
- Ideal für Unternehmen

🏠 Wo kommen Firewalls zum Einsatz?

Ort	Beispiel	Funktion
Router	FRITZ!Box, OPNsense	Schützt das gesamte Heimnetz
PC/Notebook	Windows-Firewall	Schützt das einzelne Gerät
Unternehmensnetzwerke	Sophos, pfSense, Fortinet	Umfassender Schutz mit Regeln, VPN, Monitoring
Server & Cloud	AWS Security Groups, Linux iptables	Regelt Zugriff auf Dienste und Ports

---

🧠 Warum brauchst du eine Firewall?

Ohne Firewall wäre dein System wie ein Haus ohne Türschloss:

🔐 Mit Firewall	🔓 Ohne Firewall
Schutz vor Hackern	Offene Angriffsfläche
Kontrolle über Netzwerkzugriffe	Jeder kann mitreden
Blockierung schädlicher Software	Ungehinderter Datenverkehr
Begrenzung von Internetzugriffen	Keine Kontrolle

Gerade **öffentliche WLANs**, **nicht aktualisierte Systeme** und **IoT-Geräte** (z. B. smarte Steckdosen) sind beliebte Angriffsziele – hier ist eine Firewall **besonders wichtig**.

📊 Beispiel für eine einfache Regel

Regel: Erlaube nur Verbindungen von innen nach außen auf Port 443 (HTTPS)
✅ Webseiten aufrufen möglich
❌ Hacker von außen kommen nicht rein

⚙️ Bekannte Software- & Hardware-Firewalls

Typ	Beispiele
Software-Firewalls	Windows Defender Firewall, UFW (Linux), Comodo
Hardware-Firewalls	OPNsense, pfSense, FortiGate, Cisco ASA
Cloud-Firewalls	Azure Network Security Groups, AWS Security Groups

---

🛠️ Merksatz für Einsteiger

Eine **Firewall ist der Türsteher deines Netzwerks**: Sie lässt nur rein, wer auf der Gästeliste steht – und schmeißt den Rest raus.