

[zurück](#)

# Firewall-Arten - Stateful, Stateless, Next-Gen

Firewalls sind zentrale Sicherheitskomponenten, die den Netzwerkverkehr überwachen, filtern und kontrollieren. Es gibt verschiedene Firewall-Typen mit unterschiedlichen Fähigkeiten.

Die drei wichtigsten sind:

- Stateless Packet Filtering
- Stateful Inspection
- Next-Generation Firewalls (NGFW)

## 1. Stateless Firewall

Eine stateless Firewall prüft **jedes Paket einzeln**, ohne sich an vorherige Pakete zu erinnern. Sie kennt keine Verbindungen und keine Zustände.

### Merkmale

- arbeitet auf Layer 3 (IP) und Layer 4 (Ports)
- jedes Paket wird unabhängig beurteilt
- sehr schnell und einfach
- weniger sicher als stateful Firewalls

ASCII:

```
[Packet 1] → Entscheidung  
[Packet 2] → Entscheidung  
[Packet 3] → Entscheidung
```

### Beispielregel

```
Erlaube TCP Port 80 →  
Blockiere alles andere
```

## Nachteile

- keine Erkennung, ob Paket zu einer bestehenden Verbindung gehört
- kann leicht umgangen werden (z. B. ACK-Floods)
- keine tiefere Analyse

## Einsatz heute

- einfache ACLs auf Routern
  - sehr alte Firewalls
  - selten im Produktionsnetz
- 

## 2. Stateful Firewall (Stateful Packet Inspection)

Eine stateful Firewall merkt sich **Zustände von Verbindungen**.  
Sie weiß, ob ein Paket zu einer gültigen, bestehenden Session gehört.

### Merkmale

- Standard in modernen Firewalls
- führt eine **State Table**
- erkennt Session-Start, Session-Ende
- blockiert unerwünschte Pakete zuverlässig

ASCII:

```
[Tabelle]
192.168.1.10:443 → ESTABLISHED
192.168.1.20:22  → NEW
```

Firewall prüft Pakete anhand dieser Tabelle.

### Vorteile

- viel sicherer als stateless
- erkennt legitime vs. illegitime Pakete
- reduziert Regeln stark → „Allow outbound, block inbound“
- ideal für NAT

## Beispiel: typische Geschäftsregel

```
LAN → Internet: erlaubt  
Internet → LAN: geblockt (außer etablierte Sessions)
```

## Nachteile

- kann überlastet werden (State Table Exhaustion)
- keine tiefe Analyse auf Layer 7

## Einsatzbereiche

- Heimrouter
- Unternehmensfirewalls
- Linux iptables / nftables
- OPNsense / pfSense / FortiGate / Palo Alto

---

## 3. Next-Generation Firewall (NGFW)

NGFWs sind moderne Firewalls mit erweiterten Sicherheitsfunktionen. Sie arbeiten nicht nur auf Layer 3/4, sondern analysieren auch **Layer 7** (Anwendungen).

Bekannte Hersteller:

- Palo Alto
- FortiGate
- Sophos
- Check Point

## Merkmale einer NGFW

- Stateful Inspection
  - Deep Packet Inspection (DPI)
    - \* Applikationskontrolle (z. B. Facebook, Netflix, Teams erkennen)
    - \* Benutzerbasierte Regeln (via LDAP/AD)
    - \* TLS Inspection (Decrypt/Inspect)
    - \* integrierter Antivirus / AntiMalware
    - \* integrierter IDS/IPS
    - \* Webfilter (URL Filtering)
    - \* Sandboxing
    - \* Threat Intelligence Feeds

ASCII:

Traffic → Firewall → IDS/IPS → App-ID → User-ID → Policies → Entscheidung

## Vorteile

- extrem hohe Sicherheit
  - erkennt Anwendungen, nicht nur Ports
    - \* blockiert Malware, C2-Kommunikation, Exploits
    - \* perfekt für Unternehmen

## Nachteile

- deutlich teurer
  - Einrichtung komplexer
    - \* TLS-Inspection kann Datenschutzrelevant sein

—

## Vergleichstabelle

Typ	Erinnerung an Sessions	Tiefe Analyse	Sicherheit	Komplexität	Einsatz
Stateless	<input type="checkbox"/> nein	<input type="checkbox"/> nur Ports	niedrig	sehr gering	Router-ACLs
Stateful	<input checked="" type="checkbox"/> ja	<input type="checkbox"/> keine L7	gut	mittel	Heim, Unternehmen
NGFW	<input checked="" type="checkbox"/> ja	<input checked="" type="checkbox"/> Layer 7, IPS	sehr hoch	hoch	Unternehmen, SOC

## 4. Beispiele aus der Praxis

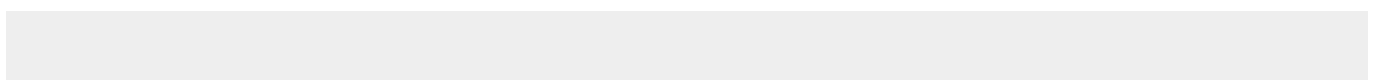
### Stateful Firewall: iptables/nftables

Linux-Firewall mit Session-Tracking:

```
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

### NGFW: Palo Alto

Regel:



Erlaube: Usergruppe "IT", App "GitHub", VLAN 10 → Internet  
Blockiere: Social Media für alle außer GF

## OPNsense / pfSense

- stateful Firewall
  - \* Suricata (IDS/IPS) integriert
  - \* URL-Filter per Plugin möglich

—

## 5. Layer-7-Erkennung - warum wichtig?

Früher:

- Port 80 = HTTP
  - \* Port 443 = HTTPS
  - \* Port 21 = FTP

Heute:

- HTTP/HTTPS tunneln ALLES
  - \* Anwendungen sind nicht mehr portgebunden
  - \* Beispiel:
    1. Teams
    2. Zoom
    3. Netflix
    4. Discord

NGFW erkennt die Anwendung → nicht nur den Port.

---

## 6. Logging & Monitoring

Firewalls erzeugen typische Logs:

- Allowed / Denied
  - Blocked inbound attempts
    - \* Portscans
    - \* IDS/IPS alerts
    - \* TLS handshake metadata
    - \* App-ID Erkennung
    - \* Benutzerzuordnung (User-ID)

—

# Zusammenfassung

- Stateless Firewalls filtern rein nach Ports/IP – kaum noch genutzt
  - Stateful Firewalls sind Standard, sie verstehen Sitzungen
  - \* NGFWs gehen darüber hinaus:
    1. Deep Packet Inspection

- IDS/IPS
- Anwendungsfiler
- Benutzerbasierte Kontrolle
- Threat Intelligence

\* Moderne Unternehmensnetze nutzen fast immer NGFWs

From: <http://wiki.nctl.de/dokuwiki/> - ☐ **Veni. Vidi. sudo rm -rf / vici.**

Permanent link: <http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:grundlagen:netzwerkdienste:firewall-arten&rev=1764777523>

Last update: **03.12.2025 16:58**

