zurück

Firewall-Grundlagen

Eine Firewall überwacht, steuert und filtert den Datenverkehr zwischen Netzwerken. Sie entscheidet, welche Verbindungen erlaubt sind und welche blockiert werden.
Firewalls sind ein zentraler Bestandteil der IT-Sicherheit.

Warum braucht man Firewalls?

- Schutz vor unerlaubten Zugriffen
- Kontrolle des ein- und ausgehenden Datenverkehrs
- Trennung von vertrauenswürdigen und untrusted Netzen
- Absicherung von Servern, Heimnetzwerken und Unternehmensnetzen
- Einhaltung von Sicherheitsrichtlinien

Arten von Firewalls

1. Paketfilter (Layer 3/4)

Analysiert:

- Quell-IP
- Ziel-IP
- Protokoll (TCP/UDP/ICMP)
- Portnummern

Beispielregel:

- Erlaube TCP Port 443 nach außen
- Blockiere eingehendes TCP Port 22

Vorteile:

- schnell
- einfach

Nachteile:

- keine Analyse des Inhalts

2. Stateful Firewall

Merkt sich Verbindungen (Session-Tracking).

Beispiel:

- Ausgangsverbindung: Port 443 erlaubt
- Rückverkehr wird automatisch akzeptiert

Standard bei:

- OPNsense
- pfSense
- FortiGate
- Windows-Firewall

3. Application Firewall (Layer 7)

Analysiert Verkehr auf Anwendungsebene:

- HTTP-Inhalte
- DNS-Abfragen
- SSL-Inspection
- spezifische URLs

Wird verwendet in:

- Web Application Firewalls (WAF)
- Cloud-Firewalls
- Next-Generation Firewalls

4. Next-Generation Firewall (NGFW)

Kombiniert:

- Stateful Firewall
- Application Control
- Intrusion Detection/Prevention (IDS/IPS)
- Antivirus/Antimalware
- SSL-Inspection
- Benutzerbezogene Regeln

Beispiele:

- FortiGate
- Palo Alto
- Sophos XG

Wichtige Begriffe

DMZ (Demilitarized Zone)

Ein separater, isolierter Bereich für öffentlich erreichbare Server.

```
Internet →[ Firewall ]→ DMZ →[ Firewall ]→ Internes LAN
```

Server in der DMZ:

- Webserver
- Mailserver
- VPN-Gateways

NAT (Network Address Translation)

Übersetzt interne private IPs zu einer öffentlichen IP.

Arten:

- SNAT (Source NAT) – ausgehend
- DNAT (Destination NAT) – eingehend
- PAT (Port Address Translation)

Whitelisting vs. Blacklisting

- Whitelist → nur Erlaubtes ist erlaubt
    - Blacklist → nur Verbotenes verboten
      * In der IT gilt: **Whitelist = sicherer**

Regeln in einer Firewall

Eine Regel besteht meist aus:

- Quelle
- Ziel
- Protokoll
- Port
- Aktion (Allow / Deny / Reject)

Beispiel:

```
Regel 1:  LAN → Internet, TCP 80/443, Allow
Regel 2:  Internet → LAN, Deny
Regel 3:  LAN → Server VLAN, Allow
```

Beispiel: Firewall-Regeln im Unternehmen

```
+----------------------+----------------------+-------------+
| Quelle               | Ziel                 | Aktion      |
+----------------------+----------------------+-------------+
| VLAN 10 Clients      | Internet             | Allow 80/443|
| VLAN 10 Clients      | Server VLAN          | Allow SMB   |
| Internet             | LAN                  | Deny        |
| DMZ Webserver        | LAN Datenbank        | Allow 3306  |
+----------------------+----------------------+-------------+
```

Stateful vs Stateless

Feature	Stateless	Stateful
——————————-	————————-	————————-
Merkt sich Verbindungen	Nein	Ja
Performance	Hoch	Hoch
Sicherheit	Mittel	Hoch
Beispiel	iptables raw	pf / OPNsense

Intrusion Detection & Prevention

Firewalls können zusätzlich IDS/IPS integrieren:

- Suricata
    - Snort
      * FortiGuard Signaturen

  Diese analysieren Anomalien im Traffic und können Angriffe erkennen/blockieren:

- Portscans
    - DoS/DDoS
      * Malware
      * C2-Kommunikation
      * Webshells

ASCII-Visualisierung Firewall-Konzept

```
                +----------------------+
Internet  ----->|      Firewall        |-----> Internes LAN
                | Ingress / Egress     |
                +----------------------+
```

Wichtige Ports für Firewalls

- 80/443 – Web
- 22 – SSH
- 53 – DNS
- 25/587 – SMTP
- 993/143 – IMAP
- 3389 – RDP
- 5060 – VoIP
- 51820 – WireGuard

Best Practices

- Verweigern als Standard (Deny All)
- Nur benötigte Ports öffnen
- Logging aktivieren
- DMZ für öffentlich erreichbare Dienste
- Trennung von Management-Netzen
- IDS/IPS aktivieren
- regelmäßige Updates
- Backup der Konfiguration

Zusammenfassung

Firewalls schützen Netzwerke, indem sie Verkehr filtern und Regeln durchsetzen.
Es gibt verschiedene Typen (Packet Filter, Stateful, NGFW).
Sie arbeiten typischerweise mit IPs, Ports, Protokollen und Sessions.
Eine Firewall ist unverzichtbar für jedes sichere Netzwerk.

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:netzwerktechnik:firewall&rev=1764344663

Last update: **28.11.2025 16:44**