Firewall-Regeln

Inhaltsverzeichnis

Firewall-Regeln definieren, welcher Netzwerkverkehr erlaubt oder blockiert wird. Sie sind ein grundlegendes Werkzeug, um Dienste zu schützen und Angriffsflächen zu reduzieren.

Firewall-Regeln steuern Verbindungen anhand von Kriterien wie Quelle, Ziel, Port, Protokoll und Richtung. Sie bilden eine zentrale Schutzschicht für Server, Netzwerke und Anwendungen.

1 Grundprinzip

Viele Firewalls arbeiten mit einer Default-Policy und gezielten Ausnahmen.

- **Allowlist:** nur notwendige Verbindungen erlauben.
- **Deny:** nicht benötigten oder unerwünschten Verkehr blockieren.
- **Reihenfolge:** Regeln werden oft nacheinander ausgewertet.

2 Typische Regeln

Regeln sollten möglichst klar und nachvollziehbar sein.

- SSH nur für bekannte Quellnetze erlauben.
- Webdienste auf Port 80 und 443 freigeben.
- Datenbanken nicht öffentlich erreichbar machen.

3 Betrieb und Pflege

Firewall-Regeln müssen dokumentiert und regelmäßig geprüft werden.

- Alte Ausnahmen entfernen.
- Änderungen testen, bevor produktive Zugänge getrennt werden.
- Logs für Fehlersuche und Sicherheitsanalyse nutzen.

4 Fazit

Gute Firewall-Regeln sind einfach, dokumentiert und restriktiv. Sie schützen Dienste, ohne den Betrieb unnötig zu verkomplizieren.