Zugersee

Combined Networks GmbH

Open-Source-Firewall

V E R G L E I C H

Combined Networks GmbH

Löberenstrasse 10

CH-6300 Zug - Schweiz

Version	Datum	Bemerkungen
0.1	*08.11.2025*	*Entwurf*
0.2	*10.11.2025*	*Hinzugefügt: Kapitel Security Fabric*

Inhaltsverzeichnis

Vergleichs- und Beratungsbericht: OPNsense vs. pfSense

Entscheidungshilfe für den Einsatz einer Open-Source-Firewall im Unternehmensumfeld

Einführung: Warum eine Open-Source-Firewall?

Im Bereich Netzwerksicherheit setzen immer mehr Unternehmen auf Open-Source-Firewalls anstelle proprietärer, kommerzieller Systeme.

Die Gründe sind vielfältig und lassen sich sowohl aus sicherheitstechnischer als auch aus wirtschaftlicher Perspektive begründen:

- **Transparenz und Nachvollziehbarkeit:** Bei Open-Source-Lösungen steht der Quellcode vollständig offen. Dadurch ist nachvollziehbar, welche Funktionen implementiert sind und welche Daten verarbeitet oder übermittelt werden. Dies reduziert das Risiko von «Black-Box»-Verhalten oder versteckten Telemetrie-Komponenten, wie sie in manchen proprietären Produkten vorkommen.
- **Sicherheitsvertrauen durch Community-Audit:** Da viele internationale Experten und Institutionen den Code einsehen und regelmässig prüfen, werden Schwachstellen oft schneller erkannt und behoben. Sicherheitsupdates erscheinen meist zeitnah und transparent dokumentiert.
- **Unabhängigkeit von Herstellerbindung (Vendor Lock-in):** Der Betrieb, die Wartung und Erweiterung können unabhängig vom ursprünglichen Hersteller erfolgen. Das Unternehmen behält somit die Kontrolle über Technologie, Updates und Lebenszyklen.
- **Kostenoptimierung und Flexibilität:** Open-Source-Firewalls erlauben den Einsatz auf Standardhardware oder virtuellen Maschinen. Lizenzkosten entfallen weitgehend; stattdessen wird gezielt in Hardware, Support oder Consulting investiert.
- **Datenschutz und Compliance:** Gerade im Schweizer Umfeld ist es wichtig, die Datenhoheit zu behalten. Schweizer Unternehmen unterliegen dem Datenschutzgesetz (DSG), das ähnlich wie die DSGVO hohe Anforderungen an den Umgang mit personenbezogenen Daten stellt.

Überblick: Die beiden führenden Open-Source-Firewalls

Die beiden etabliertesten Projekte im Bereich Open-Source-Firewalls sind:

- **OPNsense** – eine vollständig Open-Source-basierte Firewall-Distribution, entwickelt als Fork von pfSense, mit Fokus auf Transparenz, modernes Interface und erweiterbare Plugin-Struktur.
- **pfSense (Community Edition / pfSense Plus)** – eine seit vielen Jahren bewährte Plattform von Netgate mit stabiler FreeBSD-Basis und optionalen kommerziellen Erweiterungen.

Beide Systeme basieren auf **FreeBSD**, bieten stateful Packet Inspection, VPN, Routing, NAT, Proxy, Intrusion Detection/Prevention und umfangreiche Reporting-Funktionen.

Technische und konzeptionelle Gegenüberstellung

Open-Source-Philosophie und Lizenzmodell

OPNsense ist zu 100 % Open Source unter einer BSD-Lizenz. Alle Systemkomponenten und Plug-ins sind frei zugänglich.

pfSense bietet ebenfalls eine Open-Source-Variante («Community Edition»), hat aber mit pfSense Plus eine kommerzielle Linie eingeführt, deren Funktionen nicht vollständig offen liegen.

> Hinweis: Für Organisationen, die maximale Transparenz und Auditierbarkeit fordern (z. B. Behörden, Forschungsinstitute, kritische Infrastrukturen), bietet OPNsense das klarere Lizenzmodell ohne Herstellerabhängigkeit.

Web-Filter, Inhaltskontrolle und Sicherheitsfunktionen

Beide Systeme unterstützen URL-Filtering, DNS-Blocking und Proxy-basierte Kontrolle.

- OPNsense bietet zusätzlich eine eingebaute Funktion für DNS-Blocking nach Kategorien, die eine einfache Zwischenlösung für Webfilterung ermöglicht.
- Bei pfSense sind die klassischen Pakete für Proxy- und Content-Filterung (Squid, SquidGuard, Lightsquid) offiziell als veraltet markiert und werden in zukünftigen Major-Releases nicht mehr unterstützt.

> Für Unternehmen, die eine einfache DNS-basierte Filterung ohne zusätzliche kostenpflichtige Pakete benötigen, kann OPNsense hier die praktikablere Lösung darstellen.

VPN-Unterstützung und Fernzugriff

Beide Systeme unterstützen die gängigen Protokolle OpenVPN, IPsec und WireGuard.

- OPNsense integriert WireGuard nahtlos mit offizieller Dokumentation und GUI-basiertem Setup.
- pfSense hat ebenfalls WireGuard-Unterstützung, allerdings gab es zeitweise Versionsprobleme nach bestimmten Updates – die Stabilität hängt von der jeweiligen Release-Version ab.

> Hinweis: Für Unternehmen mit hohem Bedarf an schnellen, sicheren Remote-Verbindungen empfiehlt sich OPNsense aufgrund der stabileren und dokumentierten WireGuard-Integration.

Intrusion Detection and Prevention (IDS/IPS)

Beide Systeme setzen auf etablierte Open-Source-Engines:

- **Suricata** – in OPNsense vollständig integriert, inklusive regelbasierter Echtzeit-Blockierung.
- **Snort / Suricata** – bei pfSense optional über Pakete installierbar.

> Hinweis: Funktionsgleichheit ist gegeben; entscheidend ist hier die Hardwareausstattung (CPU/RAM), da IDS/IPS rechenintensiv ist.

Datenschutz, Datensicherheit und Herstellervertrauen

Ein wichtiger Unterschied liegt in der Wahrnehmung der Projekte:

- OPNsense wird als unabhängige Open-Source-Community entwickelt (Deciso B.V., Niederlande).
- pfSense wird von Netgate (USA) kommerziell geführt, was zu einer gewissen Bindung an den Hersteller und dessen Appliances führt.

> Hinweis: Für Organisationen mit Privacy- und Compliance-Fokus (z. B. öffentliche Verwaltung, Forschung, Gesundheitswesen) bietet OPNsense mehr Unabhängigkeit und Kontrolle.

Zentrale Verwaltung und Integration (Security Fabric)

Kommerzielle Firewall-Hersteller wie Fortinet, Palo Alto, Sophos oder Check Point setzen seit Jahren auf stark integrierte Ökosysteme. Bei Fortinet etwa sorgt die Security Fabric für die zentrale Verwaltung von Firewalls, Access Points, Switches und Endpoint Security über eine gemeinsame Management-Plattform. Diese Systeme bieten Komfort, Übersicht und einheitliche Policy-Steuerung – sind jedoch proprietär, kostenintensiv und binden den Kunden vollständig an den Hersteller (Vendor Lock-in).

Open-Source-Ansatz: Modular statt monolithisch

Open-Source-Firewalls wie OPNsense und pfSense verfolgen bewusst einen modularen Architekturansatz. Es existiert keine proprietäre Fabric, sondern eine offene Integrationslandschaft auf Basis standardisierter Schnittstellen (REST-API, Syslog, SNMP, NetFlow). Dadurch können bestehende Tools für Logging, Monitoring und Automatisierung flexibel angebunden werden – unabhängig vom Hersteller.

OPNsense

Bietet eine vollständige REST-API, mit der Konfiguration, Reporting und Automatisierung über Tools wie Ansible, SaltStack oder Terraform erfolgen können.

Optional ermöglicht Zenarmor (kommerziell) eine cloudbasierte zentrale Richtlinien-Verwaltung mehrerer Firewalls. Datenschutztechnisch ist dies jedoch nur bedingt empfehlenswert, da es sich um eine SaaS-Lösung ausserhalb der Schweiz bzw. EU handelt.

In der Business Edition (Deciso) stehen Funktionen für zentralisierte Updates, Support-Management und Vorlagen-Verwaltung zur Verfügung.

Es existieren erste Community-Projekte (z. B. OPNhub), die den Aufbau eines zentralen Dashboards über API-Schnittstellen erlauben.

pfSense

Verfügt über eine ähnliche API-Struktur und kann ebenfalls über Infrastructure-as-Code-Tools (z.B. Ansible, Terraform) verwaltet werden.

Netgate Cloud Management (pfSense Plus) befindet sich im Aufbau und soll künftig zentrale Administration ermöglichen – ist jedoch proprietär, cloudbasiert (USA) und somit nicht datenschutzkonform im Sinne von DSG/DSGVO.

Alternativ wird häufig auf externe Systeme für Logging, Monitoring und Backup gesetzt.

Alternative zur Security Fabric

Open-Source-Firewalls können durch die Kombination mehrerer etablierter Tools eine ähnliche Funktionalität wie eine Security Fabric abbilden:

- Zentrales Monitoring: Zabbix, Prometheus, Checkmk
- Log-Management und Korrelation: ELK, Graylog, Wazuh, Security Onion
- Automatisierung: Ansible, Terraform, SaltStack
- Reporting und Dashboards: Grafana, Netdata

Ein zentrales Thema im Vergleich zwischen proprietären Security Fabrics und Open-Source-Lösungen ist die Verwaltung von Netzwerkkomponenten wie Switches und Access Points. Während Anbieter wie Fortinet oder Palo Alto hier geschlossene Systeme mit enger Produktbindung einsetzen, bietet sich im europäischen Umfeld die Kombination aus Open-Source-Firewall (z.B. OPNsense/pfSense) und LANCOM-Netzwerkkomponenten als datenschutzfreundliche Alternative an.

Für LANCOM Systems ist digitale Souveränität sowohl eine wichtige Verpflichtung als auch eine persönliche Mission. Als deutscher Hersteller von Netzwerktechnologie mit Produktion und Entwicklung in Deutschland und einem besonderen Fokus auf Backdoor-Freiheit und Datenschutz will LANCOM mit sicheren, selbstbestimmten Produkten und sozialem Engagement die digitale Souveränität in Europa fördern.

Diese Kombination ermöglicht eine offene, skalierbare und datenschutzkonforme Architektur, ohne Bindung an einen einzelnen Hersteller. Der Integrationsaufwand ist zwar höher, bietet aber langfristig grössere Transparenz, Flexibilität und Unabhängigkeit – ein wichtiger Aspekt, insbesondere im Schweizer Umfeld mit hohen Anforderungen an Datensouveränität und Cloud-Act-Freiheit.

Systemanforderungen und Skalierung

Einsatzgrösse	Empfohlene Hardware	Hinweise
Kleine Netzwerke / Home-Office ca. 10–20 Clients	Dual-Core CPU ≥1 GHz, 2–4 GB RAM, 8–32 GB SSD	Für NAT/VPN ausreichend, ohne IDS/UTM
KMU ca. 50–200 Clients	4–6 Cores, 8–16 GB RAM, 120 GB SSD, Intel NICs	Ideal für UTM, Webfilter, VPN
Unternehmen >200 Clients	6–8 Cores, 16–64 GB RAM, NVMe SSD ≥240 GB, 10 GbE NICs	Für TLS-Inspection, IDS/IPS, umfangreiches Logging
Virtualisierte Umgebung	≥2 vCPU, ≥4 GB RAM, 20–40 GB Disk	Beide Systeme virtualisierbar

Hinweis: Beide Firewalls laufen zuverlässig auf Standard-x86_64-Hardware oder Virtualisierungsplattformen. Entscheidend ist der Treibersupport durch FreeBSD, insbesondere bei Netzwerkkarten.

Management, Erweiterbarkeit und Support

OPNsense bietet ein modernes Webinterface mit Plug-in-Store. Erweiterungen (z. B. Zenarmor, WireGuard, Suricata) lassen sich direkt über die GUI aktivieren.

pfSense verfügt über eine bewährte, aber klassischere Oberfläche; Erweiterungen werden manuell über Paketverwaltung installiert.

Support und Updates:

- OPNsense veröffentlicht regelmässig Sicherheits- und Funktionsupdates mit transparentem Changelog.
- pfSense bietet Enterprise-Support direkt über Netgate; für pfSense Plus sind kommerzielle Serviceverträge verfügbar.

Hinweis: Unternehmen mit internem Know-how und Wunsch nach Selbstverwaltung profitieren eher von OPNsense; wer Hersteller-Support benötigt, greift zu pfSense Plus.

Betrieb, Sicherheit und Wartung

Beide Systeme bieten vergleichbare Sicherheitsmechanismen:

- Stateful Firewall, NAT, VLAN, Multi-WAN, Captive Portal
- VPN-Gateway, IDS/IPS, Geo-Blocking, DNS-Filter
- Backup und High Availability über CARP/State Sync

Empfohlen wird:

- Regelmässige Konfigurations-Backups
- Update-Tests in Staging-Umgebungen
- Monitoring über Syslog, Graylog oder ELK
- Einsatz von AES-NI-fähigen CPUs für verschlüsselten VPN-Traffic

Datenschutz und Compliance (DSG)

Ein grosser Vorteil von Open-Source-Firewalls liegt in der **datenhoheitlichen Selbstverwaltung**:

- Keine automatischen Cloud-Log-Uploads
- Kein Zwangsaccount beim Hersteller
- Auditierbarkeit der Datenverarbeitung
- Konfigurierbare Retention für Logs und Monitoring

Gerade im öffentlichen Bereich und in sensiblen Sektoren (Gesundheit, Bildung, Verwaltung) wird diese Offenheit zunehmend gefordert oder vorgeschrieben.

Kompatibilität mit Hardware / IPU Systems

Beide Firewalls basieren auf FreeBSD und unterstützen gängige Intel- und AMD-Hardware.

Wenn IPU Systems auf eine bestimmte Appliance oder industrielle Plattform verweist, gilt:

Läuft FreeBSD darauf, läuft auch OPNsense bzw. pfSense.

Insbesondere Intel-NICs (igb/ix/ixl-Treiber) werden empfohlen; Realtek-NICs sind nur bedingt stabil.

Zusammenfassung und Empfehlung

Bewertungskriterium	OPNsense	pfSense
Lizenz und Offenheit	★★★★★	★★★★
Webfilter und UTM	★★★★★	★★★★
VPN und WireGuard	★★★★★	★★★★
Benutzerfreundlichkeit	★★★★★	★★★
Datenschutz und Herstellerneutralität	★★★★★	★★★
Hersteller-Support	★★★	★★★★★
Gesamtbewertung	**9.5 / 10**	**8.5 / 10**

Empfehlung:

Für Organisationen, die maximale Transparenz, Flexibilität und moderne Webfilterfunktionen wünschen, ist OPNsense die strategisch zukunftssichere Wahl.

pfSense bleibt eine stabile und bewährte Alternative, insbesondere wenn direkter Hersteller-Support und dedizierte Appliances (z. B. Netgate) benötigt werden.

Schlusswort

Open-Source-Firewalls wie OPNsense und pfSense stellen eine ausgereifte, sichere und kosteneffiziente Alternative zu kommerziellen UTM-Systemen dar.

Im direkten Vergleich überzeugt OPNsense durch:

- Vollständige Offenheit und Transparenz
- Moderne Architektur und benutzerfreundliche GUI
- Aktives Plug-in-Ökosystem (Zenarmor, Suricata, WireGuard)
- Hohe Datenschutz- und Compliance-Konformität.

Damit eignet sich OPNsense besonders für Organisationen, die **Sicherheit, Datenschutz und Kostenkontrolle** in den Vordergrund stellen — ohne Abhängigkeit von proprietären Anbietern.