Lago di Zugo

Combined Networks GmbH

Firewall open source

C O M P A R A Z I O N E

Combined Networks GmbH

Löberenstrasse 10

CH-6300 Zugo - Svizzera

Versione	Data	Note
0.1	08.11.2025	Bozza
0.2	10.11.2025	Aggiunta: capitolo Security Fabric

Indice

Rapporto di consulenza: OPNsense vs. pfSense

Documento di riferimento per la scelta di un firewall open source in ambiente aziendale

Introduzione: perché scegliere un firewall open source

Nel campo della sicurezza di rete, un numero crescente di aziende sceglie firewall open source invece di soluzioni proprietarie o commerciali.

Le ragioni sono molteplici e riguardano sia la sicurezza sia l'aspetto economico e strategico.

1. **Trasparenza e verificabilità:** con le soluzioni open source, il codice sorgente è completamente accessibile. Ciò consente di verificare come sono implementate le funzioni e come vengono trattati i dati, riducendo il rischio di componenti «black box» o di telemetria nascosta.
2. **Sicurezza attraverso l'audit della community:** poiché esperti e istituzioni di tutto il mondo esaminano il codice, le vulnerabilità vengono scoperte e risolte più rapidamente. Gli aggiornamenti di sicurezza sono tempestivi e documentati in modo trasparente.
3. **Indipendenza dal fornitore (Vendor Lock-in):** gestione, manutenzione e aggiornamenti possono essere effettuati senza vincolo da parte del produttore originale. L'azienda mantiene così il controllo totale sulla tecnologia e sui cicli di vita.
4. **Ottimizzazione dei costi e flessibilità:** i firewall open source possono essere installati su hardware standard o in ambienti virtualizzati, eliminando costi di licenza e consentendo di investire solo in hardware o supporto.
5. **Protezione dei dati e conformità: p**roprio nel contesto svizzero è importante mantenere la sovranità sui dati. Le aziende svizzere sono soggette alla legge sulla protezione dei dati (LPD), che, analogamente al GDPR, impone requisiti elevati in materia di trattamento dei dati personali.

Panoramica: le due principali soluzioni open source

I due progetti di riferimento nel settore dei firewall open source sono:

- **OPNsense** – distribuzione completamente open source, nata come fork di pfSense, con particolare attenzione alla trasparenza, interfaccia moderna e sistema modulare di plugin.
- **pfSense (Community Edition / pfSense Plus)** – piattaforma stabile e consolidata, sviluppata da Netgate, con opzioni di supporto commerciale.

Entrambe si basano su **FreeBSD** e offrono funzioni di firewall stateful, VPN, routing, NAT, proxy, rilevamento/prevenzione intrusioni e funzioni di rapporti avanzate.

Confronto tecnico e concettuale

Filosofia open source e licenza

OPNsense è completamente open source (licenza BSD). Tutti i componenti e plugin sono pubblici.

pfSense dispone di una versione open source («Community Edition»), ma la versione pfSense Plus include parti proprietarie.

> Per organizzazioni che richiedono massima trasparenza e verificabilità del codice, OPNsense rappresenta la scelta più coerente e libera da vincoli commerciali.

Filtro web, controllo contenuti e sicurezza

Entrambi i sistemi supportano il filtro URL, il blocco DNS e il controllo basato su proxy.

- OPNsense offre inoltre una funzione integrata di blocco DNS per categorie, che rappresenta una soluzione intermedia semplice per il filtro web.
- In pfSense, i pacchetti classici per il proxy e il filtro dei contenuti (Squid, SquidGuard, Lightsquid) sono ufficialmente considerati obsoleti e non saranno più supportati nelle future versioni principali.

> Per le aziende che necessitano di un filtro basato su DNS semplice senza pacchetti aggiuntivi a pagamento, OPNsense può risultare la soluzione più pratica.

VPN e accesso remoto

Entrambi i sistemi supportano OpenVPN, IPsec e WireGuard.

- OPNsense integra nativamente WireGuard con configurazione grafica e documentazione completa.
- pfSense supporta WireGuard, ma la community ha segnalato in passato alcuni problemi di stabilità in specifiche versioni successive agli aggiornamenti.

> Per implementazioni VPN sicure e stabili, OPNsense risulta generalmente più lineare nella configurazione.

Intrusion Detection and Prevention (IDS/IPS)

Entrambi utilizzano motori open source collaudati:

- **Suricata**: completamente integrato in OPNsense, con blocco in tempo reale e dashboard grafica.
- **Snort / Suricata**: disponibili come pacchetti opzionali su pfSense.

> In termini di funzionalità, le due piattaforme sono equivalenti; la differenza dipende dalle risorse hardware (CPU e RAM).

Sicurezza dei dati e fiducia nel produttore

Una differenza importante risiede nella percezione dei progetti:

- OPNsense è sviluppato da una comunità indipendente (Deciso B.V., Paesi Bassi).
- pfSense è gestito da Netgate (USA), con forte integrazione nella propria linea di appliance commerciali.

> Per enti pubblici o organizzazioni con requisiti di privacy, compliance e sovranità dati, OPNsense rappresenta una scelta più neutrale e controllabile.

Gestione centrale e integrazione (Security Fabric)

I produttori commerciali di firewall come Fortinet, Palo Alto, Sophos o Check Point offrono da anni ecosistemi fortemente integrati. Nel caso di Fortinet, la Security Fabric consente la gestione centralizzata di firewall, access point, switch e soluzioni endpoint tramite una piattaforma unificata. Questi sistemi garantiscono comodità e coerenza dei criteri di sicurezza, ma sono proprietari, costosi e creano un forte vincolo con il fornitore.

Approccio Open Source: architettura modulare

Le soluzioni firewall Open Source come OPNsense e pfSense adottano un approccio modulare e aperto. Non esiste una Fabric proprietaria, bensì un ecosistema di integrazione basato su API standard, Syslog, SNMP e NetFlow, che permette l'interconnessione con strumenti di logging, monitoraggio e automazione già presenti in azienda.

OPNsense

Include una REST API completa, che consente automazione e gestione tramite strumenti come Ansible, SaltStack o Terraform.

Con Zenarmor (commerciale) è possibile una gestione centralizzata cloud di più firewall, anche se con alcune limitazioni legate alla protezione dei dati (SaaS fuori dall'UE/Svizzera).

L'edizione Business (Deciso) offre supporto, gestione degli aggiornamenti e funzioni di amministrazione centralizzata.

Esistono anche progetti della community (come OPNhub) che permettono dashboard centralizzati tramite API.

pfSense

Dispone anch'esso di API e può essere integrato con strumenti di Infrastructure-as-Code come Ansible o Terraform.

La piattaforma Netgate Cloud Management (pfSense Plus) è in fase di sviluppo, ma è proprietaria e basata su cloud statunitensi, quindi non pienamente conforme al DSG/GDPR.

Molte implementazioni utilizzano soluzioni esterne per logging, monitoraggio e backup.

Alternativa alla Security Fabric

Combinando strumenti consolidati, le firewall Open Source possono offrire un livello di integrazione paragonabile a una Security Fabric proprietaria:

- Monitoraggio centralizzato: Zabbix, Prometheus, Checkmk
- Gestione log e correlazione eventi: ELK, Graylog, Wazuh, Security Onion
- Automazione: Ansible, Terraform, SaltStack
- Reporting e dashboard: Grafana, Netdata

Un aspetto chiave nel confronto tra Security Fabric proprietarie e soluzioni Open Source è la gestione di switch e access point. Mentre vendor come Fortinet o Palo Alto propongono sistemi chiusi e fortemente integrati, la combinazione di un firewall Open Source (OPNsense/pfSense) con dispositivi LANCOM rappresenta un'alternativa più trasparente e conforme alle normative europee.

Per LANCOM Systems, la sovranità digitale è sia un obbligo importante che una missione personale. In qualità di produttore tedesco di tecnologia di rete con produzione e sviluppo in Germania e un'attenzione particolare alla libertà dalle backdoor e alla protezione dei dati, LANCOM vuole promuovere la sovranità digitale in Europa con prodotti sicuri e autonomi e con un impegno sociale.

Questo approccio consente di costruire un'architettura aperta, scalabile e conforme alle normative sulla protezione dei dati, priva di vincoli di fornitore. Pur richiedendo maggiori competenze d'integrazione, offre nel lungo periodo maggiore trasparenza, flessibilità e sovranità digitale, elementi particolarmente rilevanti nel contesto svizzero.

Requisiti di sistema e scalabilità

Scenario	Hardware consigliato	Note
Piccole reti / Home Office ca. 10–20 client	CPU dual-core ≥1 GHz, 2–4 GB RAM, 8–32 GB SSD	Adeguato per NAT/VPN base
PMI ca. 50–200 client	4–6 core, 8–16 GB RAM, 120 GB SSD, NIC Intel	Ideale per UTM, filtro web, VPN
Aziende >200 client	6–8 core, 16–64 GB RAM, NVMe ≥240 GB, NIC 10 GbE	Necessario per ispezione IDS/TLS
Ambienti virtuali	≥2 vCPU, ≥4 GB RAM, 20–40 GB disco	Supportato da entrambi

Entrambi i sistemi funzionano su architettura x86_64 e in ambienti virtualizzati. È fondamentale verificare la compatibilità dei driver FreeBSD, soprattutto per le schede di rete.

Gestione, espandibilità e supporto

OPNsense dispone di un'interfaccia moderna con gestione dei plugin direttamente dalla GUI (Zenarmor, WireGuard, Suricata, ecc.).

pfSense utilizza una struttura più tradizionale, con installazione manuale dei pacchetti.

Supporto e aggiornamenti:

- OPNsense rilascia aggiornamenti frequenti e documentati.
- pfSense offre supporto commerciale diretto tramite Netgate e contratti Enterprise per pfSense Plus.

Per aziende che gestiscono internamente la sicurezza IT, OPNsense è più flessibile; per aziende che richiedono supporto vendor ufficiale, pfSense Plus rimane un'opzione solida.

Operatività e manutenzione

Funzioni di sicurezza comuni:

- Firewall stateful, NAT, VLAN, Multi-WAN, Captive Portal
- Gateway VPN, IDS/IPS, blocco geografico, filtro DNS
- Backup automatici e High Availability tramite CARP

Raccomandazioni operative:

- Backup periodici della configurazione
- Test di aggiornamento in ambiente di test
- Monitoraggio tramite Syslog, Graylog o ELK
- CPU con supporto AES-NI per migliorare le prestazioni VPN

Privacy e conformità (LPD)

Un vantaggio fondamentale dei firewall open source è la **piena sovranità sui dati**:

- Nessun invio automatico di log a servizi cloud
- Nessun account obbligatorio presso il produttore
- Possibilità di audit del trattamento dei dati
- Conservazione dei log configurabile internamente

Per enti pubblici, sanità e istruzione, questi aspetti sono ormai un requisito di conformità.

Compatibilità hardware / IPU Systems

Entrambi i firewall si basano su FreeBSD e supportano hardware Intel e AMD standard.

Se «IPU Systems» indica una piattaforma integrata o industriale specifica, la regola è:

se FreeBSD è supportato, anche OPNsense e pfSense funzionano correttamente.

È consigliabile l'uso di schede di rete Intel (driver igb/ix/ixl); i chipset Realtek sono meno affidabili per uso intensivo.

Sintesi e raccomandazione finale

Criterio	OPNsense	pfSense
Licenza e apertura	★★★★★	★★★★
Filtro web e UTM	★★★★★	★★★★
VPN e WireGuard	★★★★★	★★★★
Facilità d'uso	★★★★★	★★★
Privacy e indipendenza	★★★★★	★★★
Supporto commerciale	★★★	★★★★★
Valutazione complessiva	**9.5 / 10**	**8.5 / 10**

Raccomandazione:

Per chi privilegia trasparenza, flessibilità e funzioni avanzate di filtro web, OPNsense è la scelta più moderna e sostenibile.

pfSense resta una piattaforma robusta e consolidata, consigliata a chi necessita di supporto diretto dal produttore.

Conclusione

I firewall open source come OPNsense e pfSense offrono oggi un livello di sicurezza, stabilità e prestazioni comparabile (e in molti casi superiore) ai sistemi commerciali.

Nel confronto diretto, OPNsense si distingue per:

- Codice completamente open source e trasparente
- Interfaccia moderna e intuitiva
- Ecosistema di plugin attivo (Zenarmor, Suricata, WireGuard)
- Conformità e controllo sui dati

Per organizzazioni orientate a sicurezza, privacy e sostenibilità dei costi, OPNsense rappresenta la scelta strategicamente più vantaggiosa.