FHV
Vorarlberg University
of Applied Sciences

Open-Source-Firewalls als kosteneffiziente Sicherheitsalternative für KMU

Ein technischer und wirtschaftlicher Praxisvergleich zwischen Open Source und kommerziellen Firewall Anbietern

Bachelorarbeit

zur Erlangung des akademischen Grades

Bachelor of Science in Engineering (BSc)

Fachhochschule Vorarlberg

Software and Information Engineering

Betreut von

Dipl.-Ing. Armin Simma

Vorgelegt von

Lucas Hartmann

Dornbirn, 19.05.2026

Kurzreferat

Open-Source-Firewalls als kosteneffiziente Sicherheitsalternative für KMU

Aufgrund steigender Gefahren durch Cyberbedrohungen, verschärften gesetzlichen Security-Vorgaben und begrenzter IT-Budgets stehen kleine und mittlere Unternehmen (KMU) vor der Herausforderung, wirtschaftliche und leistungsstarke Sicherheitsarchitekturen effizient zu realisieren. Die vorliegende Bachelorarbeit untersucht, inwieweit Open-Source-Firewall-Lösungen eine technisch gleichwertige und ökonomisch attraktive Alternative zu etablierten Firewall-Lösungen wie Sophos oder FortiGate anbieten.

Im Fokus der Untersuchung liegen dabei die beiden Open-Source-Lösungen OPNsense und pfSense, da diese sowohl durch ihre technologische Reife, die Unterstützung von Enterprise-Funktionen wie Hochverfügbarkeit, als auch durch die Verfügbarkeit kommerzieller Support-Strukturen die Anforderungen an einen stabilen und sicheren Unternehmenseinsatz erfüllen. Nach einer ausführlichen Analyse dieser beiden Produkte wird, die für den KMU-Einsatz am besten geeignete Lösung identifiziert und einer intensiven technischen Prüfung unterzogen.

Die methodische Untersuchung vereint eine gründliche Literatur- und Konfigurationsanalyse mit spezifischen Praxis-Tests, um Sicherheits-Features unter realen Bedingungen zu bestätigen. Eine umfassende Kosten-Nutzen-Bewertung bildet den Kern der Arbeit. Bei diesem Vergleich werden Open-Source-Ansätze direkt mit den aktuellen Preismodellen führender Anbieter wie Sophos (Hardware- und Lizenzkosten) verglichen, wobei auch zusätzliche Faktoren wie Wartungsaufwand und Support-Strukturen in die Bewertung einfließen.

Die Arbeit soll eine gut begründete Entscheidungshilfe hervorbringen, die IT-Dienstleistenden und KMU demonstriert, ob und unter welchen Rahmenbedingungen Open-Source-Lösungen die IT-Sicherheit maximieren und gleichzeitig die Betriebskosten nachhaltig reduzieren können.

Schlagwörter: IT-Sicherheit, Open-Source-Firewall, OPNsense, pfSense, KMU (Kleine und mittlere Unternehmen), Kosten-Nutzen-Analyse, Netzwerksicherheit, Cyber-Risiken

Abstract

Open-Source Firewalls as a Cost-Efficient Security Alternative for SMEs

Today, increasing cyber risks, stricter regulatory requirements and limited IT budgets challenge small and medium-sized enterprises (SMEs) to implement high-performance security architectures in a practical and economical way. This bachelor thesis investigates to what extent open-source firewall solutions represent a technically equivalent and economically attractive alternative to established providers such as Sophos or FortiGate.

The study focuses on the solutions OPNsense and pfSense, as they meet the requirements for stable and secure corporate use through their technological maturity, support for enterprise features such as High Availability, and the availability of commercial support structures. After an extensive analysis, the solution best suited for SME deployment is identified and will be going through technical testing.

The methodological investigation combines detailed literature and configuration analysis with practical tests to validate security features under real-world conditions. The core of the thesis is a comprehensive cost-benefit assessment. In this process, open-source approaches are directly compared with current pricing models of market leaders like Sophos (hardware and licensing costs), while also incorporating other factors such as maintenance effort and support structures.

The result of this work is a well-founded decision support that demonstrates to IT service providers and SMEs the conditions under which open-source solutions can maximize IT security while sustainably minimizing operating costs.

Keywords: IT Security, open-source Firewall, OPNsense, pfSense, SME (Small and Medium-sized Enterprises), Cost-Benefit Analysis, Network Security, Cyber Risks

Inhaltsverzeichnis

Inhaltsverzeichnis 4

Darstellungsverzeichnis 6

Tabellenverzeichnis 7

1. Einleitung 8

1.1 Motivation und Problemstellung 8

1.2 Zielsetzung der Arbeit 8

1.3 Methodik und Aufbau der Untersuchung 9

2. Anforderungsprofil für Firewall-Systeme in KMU 10

2.1 Technische Anforderungen 10

2.1.1 Performance und Durchsatz 11

2.1.2 VPN 11

2.1.3 IDS und IPS 12

2.1.4 Application Control und Webfilter 12

2.2 Rechtliche Rahmenbedingungen 13

2.2.1 DSGVO 13

2.2.2 NISG 2026 13

2.3 Betriebliche Anforderungen 14

2.3.1 Administrative Effizienz und Usability 14

2.3.2 Kontinuität und Hochverfügbarkeit 14

2.3.3 Monitoring, Reporting und Alerting 15

2.3.4 Wartbarkeit und Lifecycle-Management 15

2.3.5 Support-Strukturen und Ecosystem 16

3. Analyse der Open-Source-Kandidaten: pfSense und OPNsense 17

3.1 Nutzwertanalyse 19

3.2 Begründung und Bewertung 20

3.3 Auswahl der Fokus-Lösung für die Praxis-Evaluation 24

4. Evaluation im Praxisvergleich: OPNsense vs. Sophos XGS 25

4.1 Methodik und Rahmenbedingungen 25
4.2 Technischer Funktionsvergleich 26
4.2.1 DPI & TLS-Inspection 27
4.2.2 IDS und IPS 29
4.2.3 Webfilter 34
4.2.4 Konnektivität 38
4.3 Administration und Incident-Management 40
4.3.1 Dashboard-Visualisierung und Alerting 40
4.3.2 Logging-Tiefe und Monitoring 42
4.4 Wartbarkeit und Supply-Chain-Sicherheit 44
4.4.1 Patch-Management und Reaktionszeiten 44
4.4.2 Supply-Chain-Transparenz 45
5. Wirtschaftlichkeitsanalyse 46
5.1 TCO über 3 Jahre 46
5.1.1 Kalkulationsparameter und Annahmen 47
5.1.2 Investitionskosten (CAPEX) 47
5.1.3 Betriebskosten (OPEX) 48
5.1.4 Zusammenfassung der TCO 48
5.2 Lizenzmodelle und Subscriptions 49
5.3 Haftung & SLA 49
5.3.1 Hersteller-Support vs. Eigenverantwortung 49
5.3.2 Strategische Reinvestition der Lizenzersparnis 50
5.3.3 Haftung und Professionalisierung 50
6. Zusammenfassung und Ausblick 51
6.1 Zusammenfassung der Ergebnisse 51
6.2 Beantwortung der Forschungsfragen 52
6.3 Ausblick auf zukünftige Arbeiten 54
Literaturverzeichnis 55

Eidesstattliche Erklärung 58

Darstellungsverzeichnis

Abbildung 1: pfSense Dashboard 21
Abbildung 2: OPNsense Dashboard 22
Abbildung 3: SSL/TLS Regeln im Sophos Web-Admin 27
Abbildung 4: os-squid Plugin in OPNsense 28
Abbildung 5: CA Zertifikat in OPNsense 28
Abbildung 6: Squid Web Proxy Administration 29
Abbildung 7: IPS Policies im Sophos Web-Admin 30
Abbildung 8: OPNsense IPS Administration 31
Abbildung 9:OPNsense IPS Regelwerk Download 31
Abbildung 10: Blockierter Curl Befehl mit EICAR- Testdatei 32
Abbildung 11: OPNsense IPS blockiert EICAR- Testdatei 32
Abbildung 12: Sophos IPS blockiert EICAR- Testdatei 32
Abbildung 13: Kategorien-Übersicht in einer Sophos Web Policy 34
Abbildung 14: OPNsense installierte Plugins 35
Abbildung 15: Die Zenarmor Policy-Konfiguration in OPNsense 35
Abbildung 16: OPNsense blockierte Website 36
Abbildung 17: OPNsense Logs mit blockierter Website 36
Abbildung 18: Sophos blockierte Website 37
Abbildung 19: Sophos Logs mit blockierter Website 37
Abbildung 20: Sophos Remote access VPN IPsec 38
Abbildung 21: OpenVPN und weitere VPNs in OPNsense 39
Abbildung 22: Sophos Dashboard bei einem KMU 40
Abbildung 23: OPNsense Dashboard mit Plugin Widgets 41
Abbildung 24: Der Log Viewer von Sophos 42
Abbildung 25: Die Live-View-Ansicht der OPNsense Firewall 43
Abbildung 26: Die Change-Log-Historie in der OPNsense-GUI 45

Tabellenverzeichnis

Tabelle 1: Kriterien und Gewichtung für Open-Source-Firewalls 18
Tabelle 2: Nutzwertanalyse Open-Source-Firewalls 19
Tabelle 3: CAPEX Kostenvergleich Sophos und OPNsense 47
Tabelle 4: OPEX-Kostenvergleich Sophos und OPNsense 48

1. Einleitung

Diese Bachelorarbeit beschäftigt sich mit der Nutzung von Open-Source-Firewalls in kleinen und mittleren Unternehmen (KMU). Zunächst wird eine passende Open-Source-Firewall ermittelt und anschließend mit aktuellen, proprietären Firewall-Lösungen verglichen. Diese Arbeit strebt an, herauszufinden, ob Open-Source-Security-Produkte eine vollwertige Alternative für den Einsatz in Betrieben darstellen.

1.1 Motivation und Problemstellung

Die Untersuchung, ob Open-Source-Firewalls eine gleichwertige Alternative zu proprietären Systemen wie Sophos oder FortiGate darstellen, ist für die Vorarlberger Wirtschaftsstruktur von besonderer Wichtigkeit. Da in der Region viele KMU mit oft limitierten IT-Budgets angesiedelt sind, entsteht ein Konflikt zwischen knappen Ressourcen und steigenden Sicherheitsanforderungen durch Digitalisierung, steigendem Interesse am Homeoffice sowie strengeren Compliance-Vorgaben wie der DSGVO und NIS2. In diesem Kontext bieten transparente und kosteneffiziente Sicherheitslösungen die Chance, sensible Unternehmensdaten zu schützen und Ausfallzeiten zu minimieren, ohne die finanzielle Belastbarkeit der Betriebe zu überschreiten. Letztlich leistet die Wahl einer passenden Firewall-Strategie somit einen wesentlichen Beitrag zur digitalen Resilienz und langfristigen Wettbewerbsfähigkeit der regionalen Unternehmen.

1.2 Zielsetzung der Arbeit

Ziel dieser Arbeit ist es herauszufinden, ob es möglich ist, proprietäre Firewall-Systeme mit Open-Source-Lösungen zu ersetzen. Dabei sollen Kosten gespart werden, aber möglichst keine Abstriche im Bereich Sicherheit und Funktionsumfang gemacht werden. Wichtige Funktionen sollen stabil und problemlos ablaufen. Dazu zählen beispielsweise Features wie Stateful-Firewall, Segmentierung, Virtual Private Network (VPN) mit Multi-Faktor-Authentifizierung (MFA), Bedrohungen aktiv erkennen und blockieren (Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Deep Packet Inspection (DPI), Transport Layer Security (TLS)-Inspection) sowie angemessenes Protokollieren, um Datenschutz-Grundverordnung (DSGVO) und Network and Information Security (NIS) 2-Anforderungen zu erfüllen. In der Praxis sind zudem noch automatische Backups, regelmäßige Updates, ausreichende Performance, einfache Administration und hohe Verfügbarkeit entscheidend, damit Sicherheit und Betrieb stabil bleiben.

Als Ergebnis wird sich zeigen, ob und unter welchen Bedingungen es möglich und rentabel ist, sich als IT-Dienstleister*innen bei KMU für eine Open-Source-Lösung zu entscheiden.

1.3 Methodik und Aufbau der Untersuchung

Um ein präzises Ergebnis zu erzielen, folgt diese Arbeit einer wohlüberlegten Struktur und wissenschaftlichen Methodik.

Zunächst werden die aktuellen Sicherheitsstandards definiert und weitere essenzielle Anforderungen an Firewalls in KMU festgelegt. Dafür werden die derzeitige Bedrohungslage sowie die geltenden technischen Standards genau analysiert. Auf dieser Basis wird definiert, welche Funktionen dem aktuellen Stand der Technik entsprechen. Zusätzlich müssen die Firewalls wichtige rechtliche Rahmenbedingungen erfüllen, insbesondere die DSGVO und die NIS2-Richtlinie. Ebenso werden die spezifischen betrieblichen Anforderungen definiert und in das Konzept einbezogen.

Die Evaluierung der Firewall-Kandidaten OPNsense und pfSense erfolgt auf Basis zuvor definierter, zeitgemäßer Anforderungskriterien. Hierbei dient die offizielle Dokumentation beider Produkte als Grundlage, um deren Eignung für den Einsatz in KMU vergleichend gegenüberzustellen.

Die ausgewählte Firewall wird mit einem proprietären Anbieter verglichen und praktischen Tests unterzogen. Diese Tests sollen zeigen, wie sich eine Open-Source-Firewall in der Praxis im Vergleich zu proprietären Lösungen schlägt. Der Konfigurations-Umfang, die Sicherheitsfunktionen sowie die Backup- und Recovery-Möglichkeiten werden in einem Laboraufbau ausgiebig getestet und dokumentiert.

Danach wird geprüft, ob eine Open-Source-Firewall auch wirtschaftlich sinnvoll ist. Mithilfe einer ausführlichen Kosten-Nutzen-Analyse und einem direkten Preisvergleich mit einem Marktführer wird ermittelt, ob sich diese Lösung finanziell für KMU rechnet.

2. Anforderungsprofil für Firewall-Systeme in KMU

Der Stand der Technik im Bereich der Netzwerksicherheit hat sich in den letzten zehn Jahren grundlegend gewandelt. In der Vergangenheit beschränkte sich die Aufgabe von Firewall-Systemen primär darauf, Header-Informationen von Datenpaketen zu analysieren und nach festgelegten Regeln zu filtern (Paketfilterung). Diese Analyse findet hauptsächlich auf Layer 3 und 4 im OSI-Modell statt (Tanenbaum; Feamster; Wetherall 2021, S. 60).

Heutige Systeme sind jedoch längst nicht mehr nur als reine IP- und Port-Filter tätig. Um modernen Bedrohungen gerecht zu werden, müssen sie den gesamten Dateninhalt untersuchen, um komplexe Bedrohungen proaktiv zu identifizieren und zu unterbinden (BSI 2023, S. 732). Dieser Vorgang wird DPI genannt. Eine Firewall mit solchen Fähigkeiten wird auch als Next Generation Firewall (NGFW) bezeichnet (Souppaya; Scarfone 2012, S. 15). Eine NGFW operiert im Gegenzug zu der klassischen Firewall von Layer 2 bis hin zu Layer 7 übergreifend. Sie hat zusätzliche Features wie IDS/IPS, Virenscanner und Spamfilter (BSI 2023, S. 731).

In der folgenden Analyse wird untersucht, welche konkreten Anforderungen und Leistungsmerkmale ein modernes Firewall-System erfüllen muss, um in der aktuellen Bedrohungslage effektiv bestehen zu können.

2.1 Technische Anforderungen

In diesem Abschnitt werden die funktionalen Anforderungen an das Firewall-System definiert. Da DSGVO und NIS2 ein Sicherheitsniveau fordern, das dem aktuellen Stand der Technik sowie dem spezifischen Risikoprofil entspricht, müssen technische Kriterien festgelegt werden, die diese Schutzziele für KMU praktisch anwendbar macht. Um ein angemessenes Schutzniveau zu gewährleisten, werden die Anforderungen in die Bereiche Performance, Konnektivität (VPN), proaktive Abwehr (IDS/IPS) und Application- und Web-Control unterteilt.

2.1.1 Performance und Durchsatz

Die Leistungsfähigkeit einer Firewall darf die Netzwerksicherheit nicht negativ beeinflussen. Wenn die Hardware durch hohe Last überfordert ist, kann es zu Paketverlusten oder, je nach Konfiguration, zu einer Umgehung von Sicherheitsprüfungen kommen („fail-open“).

Gemäß (Hickman u.a. 2003) lässt sich Performance nicht allein durch den maximalen Durchsatz (Throughput) bestimmen, sondern muss unter realistischen Bedingungen gemessen werden. Hierzu zählen:

- **Concurrent Sessions:** Die Anzahl der gleichzeitig verwalteten Verbindungen.
- **HTTP Transfer Rate:** Die Verarbeitungsgeschwindigkeit von Anwendungsdaten.
- **Latency:** Die Verzögerung, die durch die Inspektion der Pakete entsteht.

Für die Gewährleistung der IT-Sicherheit ist der Threat-Protection-Durchsatz entscheidend. Dieser beschreibt die Performance unter der Bedingung, dass Sicherheitsfunktionen wie Antivirus- und Malware-Schutz, Logging sowie DPI simultan aktiviert sind.

Dieser Aspekt unterstreicht die unmittelbare Abhängigkeit der Software-Performance von der zugrunde liegenden Hardware-Architektur. Beim Einsatz proprietärer Firewall-Software ist zu beachten, dass die Hardware-Ausnutzung häufig durch Lizenzvorgaben limitiert wird. Ein aktuelles Beispiel hierfür ist das Sophos Firewall OS (SFOS): Während die RAM-Beschränkungen für Virtual-, Software- und Cloud-Instanzen seit dem 1. März 2025 vollständig aufgehoben wurden, bleibt die Skalierbarkeit der Hardware weiterhin an die Anzahl der lizenzierten CPU-Kerne gebunden. Die Performance der Firewall wird somit maßgeblich durch die prozessorseitige Lizenzierung (z. B. SFV4C mit 4 Kernen) definiert. („Keine RAM-Beschränkung mehr bei Sophos Virtual, Software und Cloud Firewalls – Sophos Partner News“ o. J.).

2.1.2 VPN

Ein zentrales Merkmal moderner Firewalls in KMU ist die Bereitstellung eines VPN, um die Vertraulichkeit und Integrität der Kommunikation über öffentliche Netze zu sichern (BSI 2023, S. 739).

Der (BSI 2023, S. 740) verlangt eine sorgfältige Planung von Verantwortlichkeiten und Berechtigungen sowie eine sichere Installation und Konfiguration durch qualifiziertes Personal. Zudem muss die Sicherheit der Konfiguration regelmäßig kontrolliert und nicht mehr benötigte Zugänge müssen konsequent gesperrt werden. Zur Absicherung dieser Zugänge ist eine MFA zwingend erforderlich.

2.1.3 IDS und IPS

Über den rein statischen Schutz auf Port-Ebene hinaus agieren moderne Firewalls heute Stateful. Um jedoch auch komplexe Angriffsmuster innerhalb des Datenstroms zu erkennen, ist die Ergänzung durch ein integriertes IDS/IPS essenziell. Laut (Scarfone; Mell 2007) wird empfohlen, dass das System folgende Eigenschaften beherrscht:

- Signaturbasierte Erkennung: Bekannte Angriffsmuster in Echtzeit zu identifizieren.
- Anomaliebasierte Erkennung: Abweichungen vom normalen Netzwerkverhalten zu melden, was besonders für die Abwehr von Zero-Day-Exploits relevant ist.
- DPI: Den Inhalt von Paketen bis in die Anwendungsschicht (Layer 7) zu untersuchen.

2.1.4 Application Control und Webfilter

Um dem aktuellen Stand der Technik gerecht zu werden, ist die Implementierung von Application Control und Webfilterung für KMU essenziell, da klassische Paketfilter moderne Bedrohungen auf der Anwendungsebene nicht hinreichend abdecken. Das (BSI 2023, S. 735) empfiehlt hierzu im Baustein NET.3.2.A20, Internetprotokolle wie HTTP grundsätzlich über spezifische Sicherheits-Proxys zu führen, um eine tiefgehende Untersuchung des Datenverkehrs zu ermöglichen. Da moderne Kommunikation überwiegend verschlüsselt stattfindet, betont das (BSI 2023, S. 736) in Anforderung NET.3.2.A21 die Notwendigkeit einer zeitweisen Entschlüsselung. Nur durch dieses Verfahren lassen sich Protokolle verifizieren und Datenströme wirksam auf bösartige Software untersuchen. Für Organisationen mit höherem Sicherheitsbedarf sieht das (BSI 2023, S. 737) gemäß NET.3.2.A28 zudem vor, dass potenziell gefährliche aktive Inhalte einer zentralen Filterung unterzogen werden sollen. Durch diese Maßnahmen erhalten KMU eine genaue Kontrolle über ihre Web-Applikationen, die weit über einfache Port-Sperren hinausgeht und die gesamte Angriffsfläche des Unternehmens deutlich minimiert.

2.2 Rechtliche Rahmenbedingungen

Der Einsatz einer Firewall in KMU ist in Europa keine freiwillige Maßnahme, sondern eine gesetzliche Pflicht. Dabei bilden die DSGVO und die neue NIS2-Richtlinie die rechtliche Grundlage für den technischen Schutz von IT-Systemen.

2.2.1 DSGVO

Zentral für den Einsatz von Firewalls müssen KMU gemäß („Verordnung (EU) 2016/679“ 2016, S. 32) technische Maßnahmen ergreifen, die dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessen sind. Da Vorarlberger KMU oft hoch spezialisierte Daten verarbeiten, ist eine Firewall nach dem Stand der Technik wie bereits definiert zwingend erforderlich, um die Integrität und Vertraulichkeit gemäß („Verordnung (EU) 2016/679“ 2016, S. 5) zu wahren.

2.2.2 NISG 2026

Mit dem Netz- und Informationssystemsicherheitsgesetz (NISG) („Richtlinie (EU) 2022/2555“ 2022) wurde die EU-NIS2-Richtlinie in nationales Recht überführt. Für KMU in Vorarlberg ist entscheidend, ob sie als „wesentliche“ oder „wichtige“ Einrichtung eingestuft werden. Besonders für die Vorarlberger Industrie (z.B. Maschinenbau, Elektronik) greift oft Artikel 21 des NISG 2026, der ein Risikomanagement vorschreibt. Da viele KMU als kritische Zulieferer für Großunternehmen fungieren, sind sie indirekt zur Einhaltung dieser Sicherheitsstandards verpflichtet. Die Firewall dient hierbei als zentrale Schutzmaßnahme.

2.3 Betriebliche Anforderungen

Dieses Kapitel adressiert die nicht-funktionalen Anforderungen, die über die reine Sicherheit hinausgehen und die Integration in den Geschäftsalltag sicherstellen. Darunter zählen Faktoren wie Wartbarkeit, Support-Strukturen, Monitoring und Hochverfügbarkeit.

2.3.1 Administrative Effizienz und Usability

In der modernen IT-Infrastruktur von Unternehmen sind administrative Effizienz und Usability von Firewalls keine reinen Komfortmerkmale, sondern kritische Sicherheitsfaktoren. Da Fehlkonfigurationen eine große Sicherheitslücke darstellen (BSI 2023, S. 732), ist eine intuitive Benutzeroberfläche essenziell, um eine möglichst effiziente, aber vor allem fehlerfreie Anwendung und Wartung zu gewährleisten. Eine hohe administrative Effizienz ermöglicht es IT-Dienstleistenden zudem, schneller auf Bedrohungslagen zu reagieren und den Zeitaufwand für Routineaufgaben zu minimieren. In Zeiten des Fachkräftemangels und steigender Compliance-Anforderungen wird eine einfache Firewall-Verwaltung ausschlaggebend: Sie entlastet das Personal, senkt durch optimierte Workflows die Betriebskosten und erhöht maßgeblich die Sicherheit des gesamten Unternehmensnetzwerks.

Ergänzend zur Usability der Firewall an sich, ist eine detaillierte und kontinuierlich aktualisierte Dokumentation die Grundvoraussetzung für eine fachgerechte Wartung durch IT-Dienstleister*innen. Sie dient als Wissensbasis, die sicherstellt, dass Konfigurationsentscheidungen und Regelwerksstrukturen auf Fakten statt auf Mutmaßungen basieren. Daher sollte sie gut gepflegt, aktuell und übersichtlich sein.

2.3.2 Kontinuität und Hochverfügbarkeit

Für KMU mit digitalem Geschäftsmodell stellt die Firewall eine zentrale Infrastrukturkomponente dar, deren Ausfall unmittelbar geschäftsschädigende Folgen haben kann. Um einen Single Point of Failure (SPoF) zu vermeiden, fordert der (BSI 2023, S. 737), dass Firewalls in Hochverfügbarkeits-Clustern betrieben werden sollten. Dabei kommen primär Failover-Mechanismen zum Einsatz, bei denen ein sekundäres System übernimmt, sobald die aktive Komponente eine Störung signalisiert. Diese Funktion ist oft teuer und für viele KMU nicht realistisch. Ein Open-Source Ansatz könnte ein vollwertiges Hochverfügbarkeits-Setup preiswerter ermöglichen.

2.3.3 Monitoring, Reporting und Alerting

Im Kontext der Netzwerksicherheit für KMU ist die Implementierung von Monitoring, Reporting und Alerting gemäß der Anforderung NET.3.2.A9 (BSI 2023, S. 734) nicht als optionales Zusatzfeature, sondern als integrale Betriebsvoraussetzung zu verstehen. Während das Grundschutz Kompendium eine umfassende Protokollierung (z.B. abgewiesene Verbindungen, fehlgeschlagene Authentisierungen und Konfigurationsänderungen) vorschreibt, erweitert die Standard-Anforderung NET.3.2.A23 (BSI 2023, S. 736) diesen Fokus um eine ganzheitliche Systemüberwachung. Demnach sollten Firewalls in ein umfassendes Monitoring-Konzept eingebunden werden, das die korrekte Funktion der Firewall-Dienste sowie die Einhaltung von Grenzwerten kontinuierlich überwacht. Ein automatisiertes Alerting fungiert hierbei als kritischer Multiplikator für personell begrenzte IT-Abteilungen in KMU: Es stellt die zeitnahe Benachrichtigung des Betriebspersonals bei Fehlfunktionen oder sicherheitsrelevanten Ereignissen sicher und ermöglicht es, dass Bedrohungen schnell auffallen.

2.3.4 Wartbarkeit und Lifecycle-Management

Die Wartbarkeit einer Firewall ist maßgeblich für deren langfristigen Schutz. Da KMU stetig neuen Bedrohungen ausgesetzt werden, ist ihre Einbindung in ein strukturiertes Patch- und Änderungsmanagement nach BSI-Vorgaben zwingend erforderlich.

Ein effizientes Lifecycle-Management beginnt bereits bei der Beschaffung. Hier muss sichergestellt werden, dass das Produkt langfristige Upgrade-Pfade bietet und das definierte Sicherheitsniveau über die gesamte Betriebsdauer halten kann. Ergänzt wird dies durch die Anforderung zur Notfallvorsorge, die vordefinierte Handlungsanweisungen für Hardware-Tausch oder Fehlersuche vorschreibt, um Ausfallzeiten bei Wartungsarbeiten oder Defekten zu minimieren. Gerade für KMU bietet ein systematischer Lifecycle-Ansatz die nötige Planungssicherheit, um unvorhergesehene Investitions- und Sicherheitsrisiken zu vermeiden (BSI 2023, S. 731–736).

2.3.5 Support-Strukturen und Ecosystem

Bei der Auswahl einer Firewall-Lösung, insbesondere im Open-Source-Umfeld, ist die rein technische Feature-Abdeckung nur der erste Schritt. Die langfristige Betriebssicherheit hängt maßgeblich von der Qualität und Verfügbarkeit des begleitenden Ecosystems ab. Während Open-Source-Software den Vorteil der Unabhängigkeit bietet, müssen professionelle Anwendende das Risiko fehlender direkter Haftung durch kommerzielle Support-Strukturen (SLA) absichern. Diese garantieren im Krisenfall definierte Reaktionszeiten, die für die Business Continuity essenziell sind. Häufig bieten auch Open-Source-Anbieter kommerzielle Support-Strukturen gegen Bezahlung an.

Darüber hinaus fungiert die Community-Aktivität als Indikator für die Zukunftsfähigkeit und Sicherheit des Systems: Eine aktive Community identifiziert Schwachstellen schneller und sorgt für einen kontinuierlichen Fluss an Dokumentation und Plug-ins. Ergänzt wird dieses Gefüge durch ein Netzwerk aus externen Dienstleistenden und Systemhäusern. Ein breites Ecosystem stellt sicher, dass Unternehmen nicht in eine personelle Abhängigkeit geraten, sondern auf zertifizierte Experten zurückgreifen können, die das System implementieren, warten und im Bedarfsfall skalieren können.

3. Analyse der Open-Source-Kandidaten: pfSense und OPNsense

In diesem Abschnitt werden die beiden Open-Source-Firewall-Anbieter pfSense und OPNsense verglichen. Die beiden Produkte werden nach gewichteten Kriterien bewertet und es wird festgestellt, welches Produkt besser für die Anwendung in KMU geeignet ist. Die Gewichtung der Kriterien basiert auf den Erfahrungswerten langjähriger Praxis im IT-Dienstleistungssektor für den Mittelstand. Hierbei wurden die Gewichtungsfaktoren so gewählt, dass sie die realen Bedürfnisse und Prioritäten von KMU im operativen Betrieb widerspiegeln. Der Vergleich beschränkt sich explizit auf die kostenfreien Editionen beider Plattformen: die pfSense Community-Edition von Netgate und OPNsense von Deciso. Dabei werden basierend auf den Anforderungen aus Kapitel 2 folgende Kriterien überprüft:

- Support & Gewährleistung: Gibt es kommerziellen Support (SLA und zu welchem Umfang und Preis?)
- Benutzerfreundlichkeit: Wie intuitiv ist das Web-GUI für Administrator*innen mit wenig Zeit?
- Hardware-Optionen: Bietet der Hersteller zertifizierte Appliances an? Ist es möglich, eigene Hardware zu verwenden?
- Funktionsumfang & Sicherheit: VPN (IPsec, WireGuard), IDS/IPS, Monitoring, Hochverfügbarkeit, Application Control & Webfilter.
- Update-Zyklen: Wie oft gibt es Sicherheitsupdates?

Diese Kriterien werden im Folgenden einander gegenübergestellt. Die nachstehende Tabelle fasst die gewählten Gewichtungen zusammen und liefert die entsprechende Begründung aus der Perspektive eines IT-Dienstleistungsunternehmens.

Kriterium	Gewichtung (%)	Begründung (Aus KMU-Perspektive)
Support & Gewährleistung	15%	Tritt ein Problem auf, das die interne Expertise des Dienstleistungsunternehmens übersteigt, ist der Zugriff auf eine starke Community, eine lückenlose Dokumentation oder externe Hersteller-SLAs entscheidend. Dies stellt sicher, dass komplexe Störungen schnell eskaliert und gelöst werden können, um die Ausfallzeiten beim Kunden zu minimieren.
Benutzerfreundlichkeit	20%	Da IT-Dienstleister*innen eine Vielzahl an Kundenumgebungen parallel betreuen, ist eine intuitive Bedienbarkeit entscheidend. Sie ermöglicht eine effiziente Standardisierung von Prozessen, verkürzt die Ticket-Bearbeitungszeit und minimiert das Risiko von Fehlkonfigurationen bei der Übergabe zwischen verschiedenen Technikern.
Hardware-Optionen	20%	Die Wahl zwischen vorkonfigurierten Appliances (Plug-and-Play für schnelle Implementierung) und der Nutzung vorhandener Standard-Hardware ermöglicht eine flexible Budgetplanung und eine schnelle Skalierung der Infrastruktur.
Funktionsumfang & Sicherheit	25%	Als zentrales Sicherheitsorgan muss die Firewall alle modernen Anforderungen wie sicheres Home-Office (VPN) und proaktiven Schutz (IDS/IPS) abdecken. Da dies der Kernnutzen ist, stellt dieses Kriterium die höchste Anforderung an die technische Eignung dar.
Update-Zyklen	20%	Da Cyber-Bedrohungen sich schnell entwickeln, sind regelmäßige und verlässliche Patches überlebenswichtig. Eine transparente Update-Politik garantiert nicht nur Sicherheit, sondern auch die langfristige Kompatibilität mit neuen Technologien und Compliance-Vorgaben.

Tabelle 1: Kriterien und Gewichtung für Open-Source-Firewalls

3.1 Nutzwertanalyse

Kriterium	Gewichtung (%)	pfSense	OPNsense	Gew. Wert pfSense	Gew. Wert OPNsense
Support & Gewährleistung	15%	5	6	0,75	0,90
Benutzerfreundlichkeit	20%	7	9	1,40	1,80
Hardware-Optionen	20%	8	8	1,60	1,60
Funktionsumfang & Sicherheit	25%	8	9	2,00	2,25
Update-Zyklen	20%	8	9	1,60	1,80
Gesamtsumme	100%			7,35	8,35

Tabelle 2: Nutzwertanalyse Open-Source-Firewalls

3.2 Begründung und Bewertung

Support & Gewährleistung (15%)

pfSense (5/10): Netgate bietet mit dem „Global Support“ (TAC Lite/Pro/Enterprise) ein ausgereiftes, weltweites Support-System mit festen SLA (bis zu 4h Reaktionszeit) an („Netgate Global Support“ o. J.). Dies stellt insbesondere für KMU mit kritischen Infrastrukturanforderungen eine hohe Betriebssicherheit dar. Da professionelle Support-Leistungen jedoch nicht in der Community Edition enthalten sind, ist der Nutzer hier vollständig auf die Dokumentation und Foren angewiesen („Netgate Forum“ o. J.; „pfSense Reddit Community“ o. J.).

OPNsense (6/10): Deciso bietet ebenfalls professionellen Business-Support an. Dieser ist jedoch im Vergleich zu Netgate weniger übersichtlich, auf gewisse Support-Stunden limitiert und benötigt zusätzlich eine Business-Subscription („Product categories Support“ o. J.-a). Auch hier entfallen inkludierte Support-Stunden in der freien Version. OPNsense profitiert jedoch von einer deutlich aktiveren und wachsenden Community. Dies sorgt für eine schnellere Hilfe bei Problemstellungen und eine modernere Dokumentation, was die Betriebssicherheit für das KMU ohne laufende Support-Verträge erhöht („OPNsense Forum - Index“ o. J.; „OPNsense Reddit Community“ o. J.).

Benutzerfreundlichkeit (20%)

pfSense (7/10): Die GUI ist funktional, wirkt aber im Vergleich veraltet. Die Menüführung ist historisch gewachsen und weniger intuitiv.

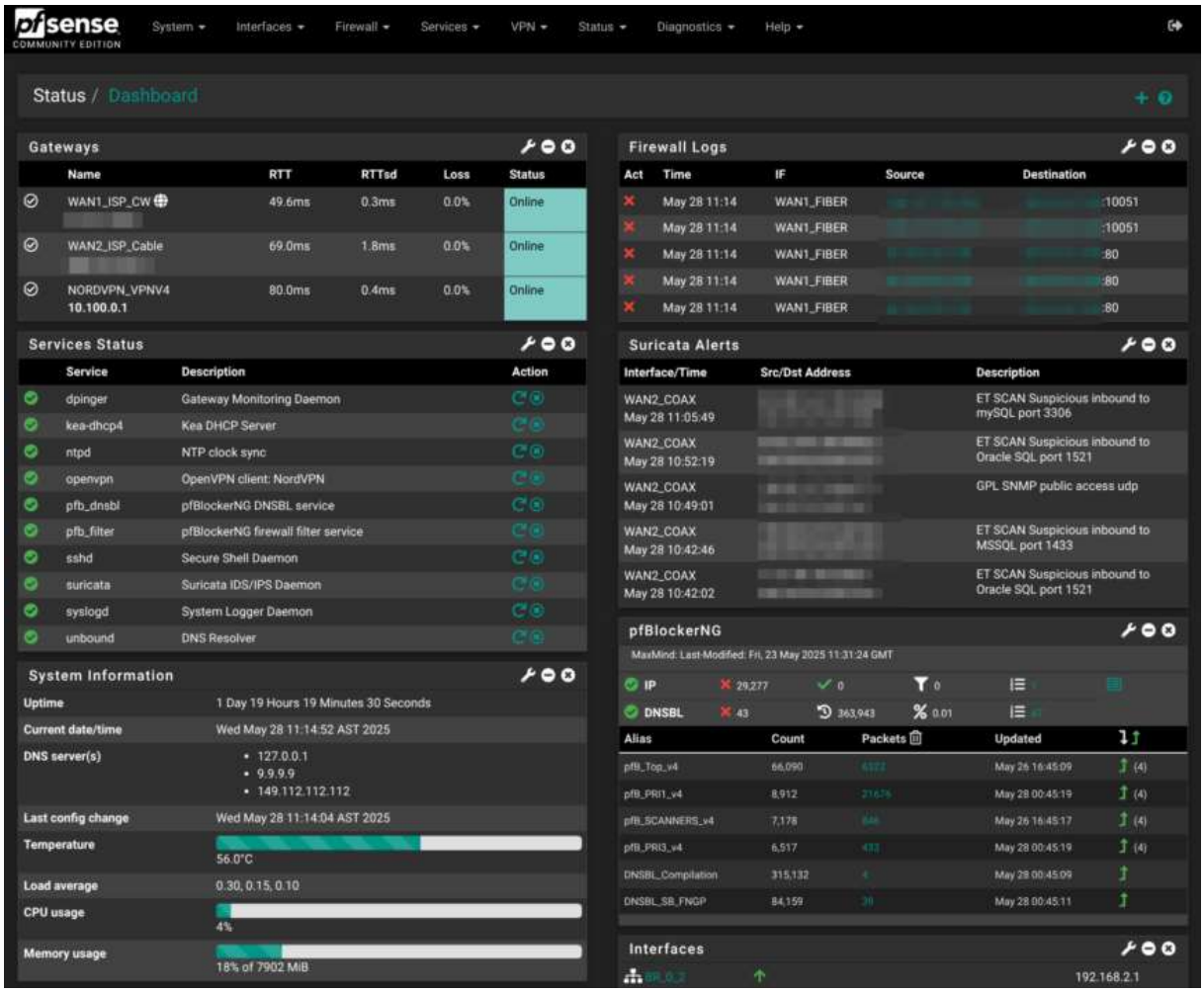


Abbildung 1: pfSense Dashboard

(James 2025)

OPNsense (9/10): Setzt auf ein modernes Bootstrap-basiertes Web-Interface. Die Suche innerhalb der GUI und das übersichtliche Dashboard machen die Verwaltung deutlich einfacher und intuitiv.

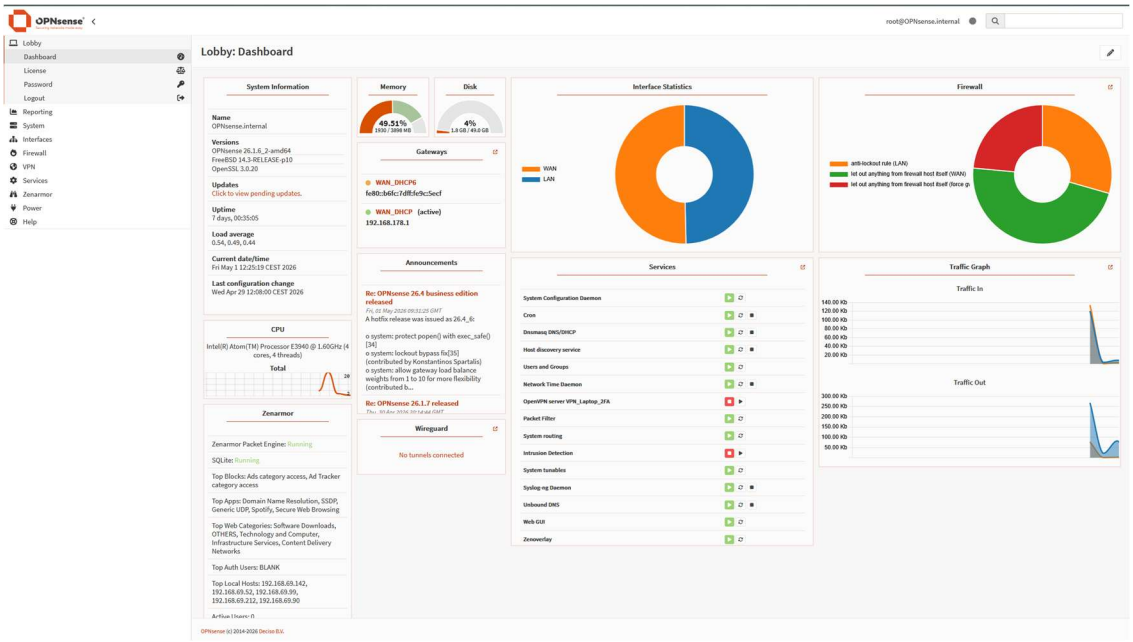


Abbildung 2: OPNsense Dashboard

Hardware-Optionen (20%)

pfSense (8/10): Netgate bietet eine sehr breite Palette an offiziellen Appliances (SG-Serie), die perfekt auf die Software abgestimmt sind. Hier ist Zero-to-Ping-Support inklusive („Netgate Store“ o. J.). Das Installieren der Software auf Drittanbieter-Hardware ist möglich, wenn diese auf der 64-Bit x86-Architektur (amd64) basiert. („Download pfSense Community Edition“ o. J.).

OPNsense (8/10): Deciso bietet ebenfalls exzellente Hardware (DEC-Serie). Die Auswahl an offiziellen Geräten ist jedoch etwas kleiner als bei Netgate („Product categories Hardware“ o. J.). Die Software kann problemlos auf eigener Hardware installiert werden. Die Architektur muss hier ebenfalls auf amd64 basieren („Download“ o. J.).

Funktionsumfang & Sicherheit (25%)

pfSense (8/10): Die Firewall bietet eine stabile Basis für Enterprise-Umgebungen und überzeugt durch eine tiefgreifende Paketverwaltung sowie robuste VPN-Lösungen wie IPsec und OpenVPN. Der Fokus liegt auf bewährten Technologien, wobei IDS/IPS oft über zusätzliche Pakete (wie Snort oder Suricata) manuell konfiguriert werden müssen („pfSense Plus Features“ o. J.).

OPNsense (9/10): Punktet durch die native Integration moderner Sicherheitsfeatures wie dem Zenarmor Plugin für NGFW-Features und einer sehr einfach zu konfigurierenden WireGuard-Implementierung. Durch die strikte Trennung von Core-System und Plugins bleibt die Angriffsfläche klein, während Features wie Zwei-Faktor-Authentifizierung (2FA) für die GUI bereits im Standard enthalten sind („OPNsense-Whitepaper-features-NIEUW.pdf“ o. J.).

Update Zyklen (20%)

pfSense (8/10): Bei den Updates wird bei pfSense ein konservativer Ansatz verfolgt. Updates erscheinen unregelmäßig, sind dafür aber sehr umfassend getestet. Ein Nachteil ist die Trennung zwischen der Plus-Version und der Community-Edition, wobei sicherheitsrelevante Patches für die Community-Edition-Version in der Vergangenheit teilweise zeitverzögert veröffentlicht wurden („Releases | pfSense Documentation“ o. J.).

OPNsense (9/10): Das Projekt zeichnet sich durch eine vorbildliche Vorhersehbarkeit aus. Es gibt zwei große Releases pro Jahr und fest eingeplante, zweiwöchentliche Sicherheits- und Stabilitätsupdates. Diese Transparenz erlaubt es den Administrierenden, Wartungsfenster präzise zu planen („Releases — OPNsense documentation“ o. J.).

3.3 Auswahl der Fokus-Lösung für die Praxis-Evaluation

Die vorliegende Nutzwertanalyse liefert eine begründete Einschätzung für die Auswahl der Firewall-Lösung. Mit einer gewichteten Gesamtsumme von 7,35 zu 8,35 Punkten (berechnet aus den Einzelbewertungen) setzt sich OPNsense gegen pfSense durch. Während beide Systeme technisch ausgereift sind und die Anforderungen eines KMU erfüllen, gaben primär die administrative Effizienz und das zukunftsweisende Software-Modell den Ausschlag für OPNsense.

Es kann also folgendes Fazit gezogen werden. Während pfSense seine Stärken in Szenarien mit strikten Support-SLA ausspielt, bietet OPNsense für den Einsatz in KMU-Umgebungen das überlegene Gesamtpaket. Die Kombination aus moderner Verwaltung, regelmäßigen Updates, hoher Transparenz und zukunftssicherer Architektur macht OPNsense zur idealen Fokus-Lösung für die weitere Praxis-Evaluation.

4. Evaluation im Praxisvergleich: OPNsense vs. Sophos XGS

Um die Eignung der OPNsense als Alternative zu kommerziellen Produkten zu bewerten, wird im Folgenden ein praxisnaher Funktionsvergleich mit der Sophos XGS durchgeführt. Der Fokus liegt dabei auf der administrativen Handhabung, dem Funktionsumfang und der Effektivität der Sicherheitsfeatures aus Sicht eines IT-Dienstleistungsunternehmens für ein KMU.

4.1 Methodik und Rahmenbedingungen

Um die OPNsense bewerten zu können, wird in diesem Kapitel ein systematischer Vergleich mit einer etablierten Enterprise-Lösung durchgeführt. Als Referenz dient hierfür eine Sophos XGS Firewall, die bereits im produktiven Einsatz bei einem Kundenumfeld implementiert und nach aktuellen Sicherheitsstandards konfiguriert ist.

Da die Hardware-Ressourcen der beiden Testumgebungen (Heimnetzwerk vs. Kundenumgebung) stark voneinander abweichen, findet kein quantitativer Leistungsvergleich (z. B. Durchsatz-Messungen) statt. Stattdessen wird eine qualitative Nutzwert-Analyse auf Basis von Anwendungsszenarien angewandt. Dabei wird untersucht, ob und mit welchem administrativen Aufwand die OPNsense in der Lage ist, die im professionellen Umfeld geforderten Sicherheits- und Verwaltungsfunktionen der Sophos XGS abzubilden.

Rahmenbedingungen der Testumgebungen:

1. Referenzsystem (Sophos XGS):
    - Umgebung: Produktives KMU-Netzwerk.
    - Konfiguration: Best-Practice-Setup durch einen externen Dienstleistungsbetrieb.
    - Zweck: Dient als Zielbild für Funktionsumfang, Benutzeroberfläche und Sicherheitsrichtlinien. Hier wird angewendet, was eine moderne Firewall leisten muss.
2. Testobjekt (OPNsense):
    - Umgebung: Kontrolliertes Heimnetzwerk.
    - Konfiguration: Manuelle Einrichtung durch den Autor, basierend auf den Anforderungen des Referenzsystems.
    - Zweck: Validierung der technischen Machbarkeit. Hier wird geprüft, wie die OPNsense die geforderten Szenarien (z. B. IDS/IPS oder Webfilter) umsetzt.

Evaluationsszenarien:

Der Vergleich konzentriert sich auf wesentlichen Säulen der Netzwerksicherheit:

- die Paketinspektion (DPI/TLS),
- die Effektivität der Angriffserkennung (IDS/IPS),
- Inhaltsfilterung (Webfilter),
- sowie die sichere Anbindung externer Beschäftigter (VPN/MFA).

Durch diese methodische Trennung wird sichergestellt, dass die Bewertung unabhängig von der zugrunde liegenden Hardware erfolgt und der Fokus rein auf der funktionalen Eignung der Software-Lösungen liegt.

4.2 Technischer Funktionsvergleich

Der folgende technische Vergleich konzentriert sich primär auf die logische Implementierung, den Funktionsumfang sowie die Konfigurationstiefe der untersuchten Sicherheitsmerkmale.

Dabei wird bewusst auf quantitative Performancemessungen (wie beispielsweise maximaler Datendurchsatz oder Pakete pro Sekunde) verzichtet. Da die OPNsense in einer Heimnetzwerk Umgebung betrieben wird, während die Sophos XGS auf dedizierter, herstellerspezifischer Hardware installiert ist, wäre ein direkter Leistungsvergleich nicht wissenschaftlich belastbar. Der Fokus dieser Evaluation liegt stattdessen auf der qualitativen Fragestellung, inwieweit die Open-Source-Lösung OPNsense in der Lage ist, die komplexen Sicherheitsanforderungen und administrativen Workflows abzubilden, die im Enterprise-Umfeld durch die Sophos XGS als Standard gesetzt werden.

4.2.1 DPI & TLS-Inspection

Da heute nahezu der gesamte Webverkehr via HTTPS verschlüsselt ist, bleibt herkömmlichen Firewalls der Inhalt der Datenpakete verborgen. Dieser Blind Spot ermöglicht es Malware, Sicherheitsmechanismen zu umgehen. Die Lösung ist TLS-Inspection, bei der die Firewall als Man-in-the-Middle (MitM) fungiert: Sie bricht die Verschlüsselung auf, scannt den Inhalt im Klartext und verschlüsselt ihn für den Client neu (BSI 2023, S. 736).

Im Folgenden wird die „Xstream-TLS-Inspection“ Funktion bei einer Sophos Firewall getestet.

Die Aktivierung erfolgt meist durch eine einzige Checkbox in der Firewall-Regel. Sophos nutzt integrierte Listen für Ausnahmen (z. B. Banking), um die Stabilität zu erhöhen. Die Aktivierung ist sehr simpel und benötigt keine weiteren Schritte.

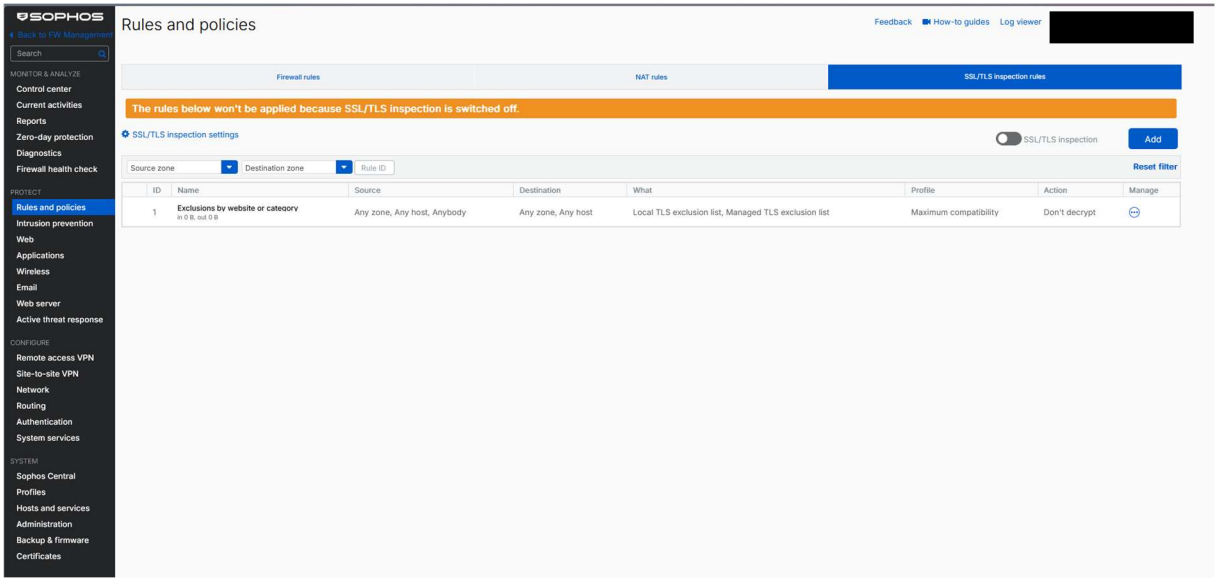


Abbildung 3: SSL/TLS Regeln im Sophos Web-Admin

Im Vergleich zu Sophos gestaltet sich die Konfiguration der DPI und der TLS-Inspection unter OPNsense komplexer. Der Prozess erfordert initial die Installation eines entsprechenden Plugins sowie die Erstellung einer Zertifizierungsstelle (CA). Erst nach der systemseitigen Aktivierung der DPI muss das generierte CA-Zertifikat manuell auf sämtlichen Endgeräten im Netzwerk als vertrauenswürdig hinterlegt werden, um eine fehlerfreie Entschlüsselung des Datenverkehrs zu gewährleisten.

1. Zuerst muss ein zusätzliches Plugin „Squid“ (os-squid) installiert werden.

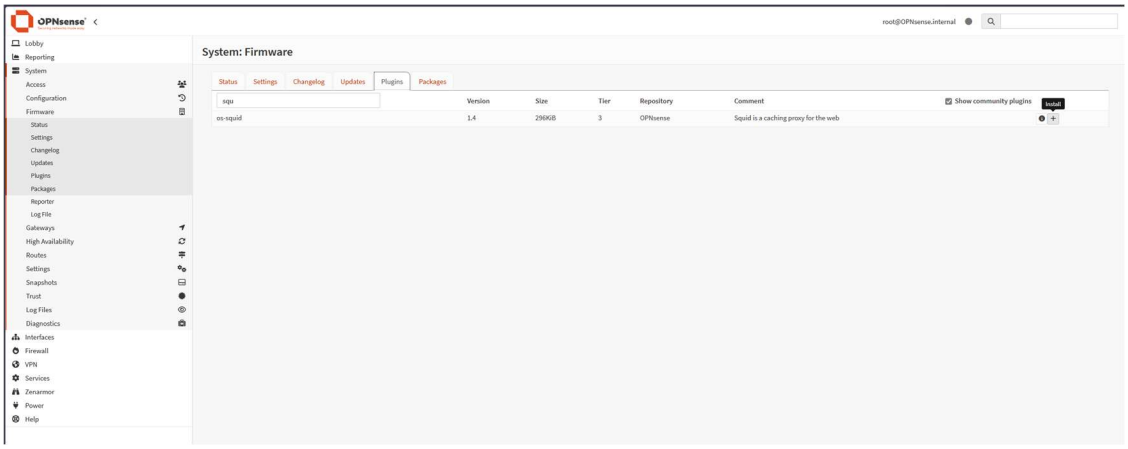


Abbildung 4: os-squid Plugin in OPNsense

2. Eine entsprechende CA kann unter *System > Trust* erstellt werden.

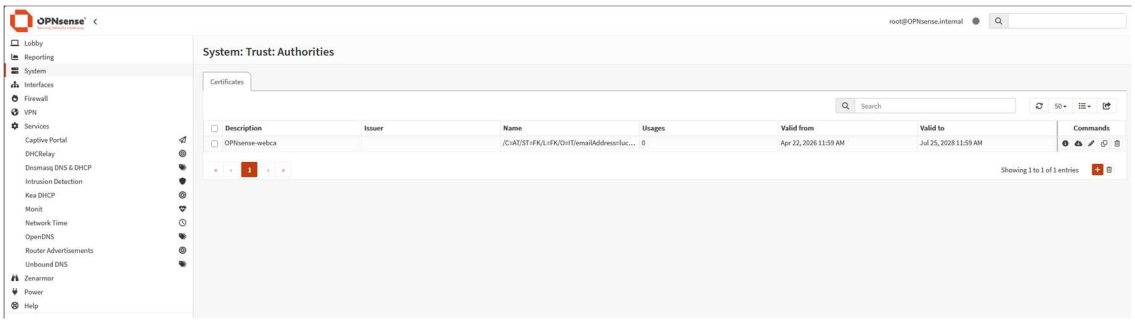


Abbildung 5: CA Zertifikat in OPNsense

3. Die „SSL Inspection“ im Proxy-Menü muss aktiviert werden.

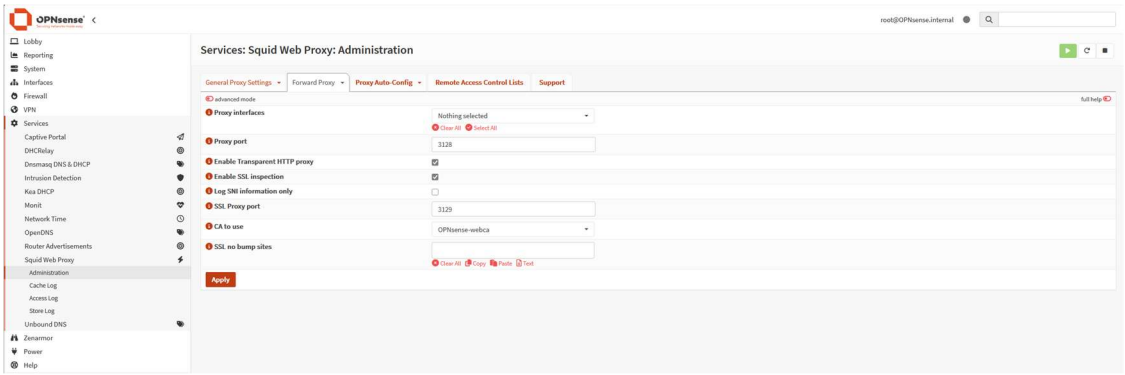


Abbildung 6: Squid Web Proxy Administration

4. Abschließend ist ein manueller Import des CA-Zertifikats in den Speicher für vertrauenswürdige Stammzertifizierungsstellen der jeweiligen Endgeräte erforderlich.

Während Sophos den Prozess durch Automatisierung und Hardwarebeschleunigung für Administrator*innen stark vereinfacht, ist die Umsetzung in OPNsense technisch anspruchsvoller und mit hohem manuellem Aufwand bei der Zertifikatsverteilung verbunden.

4.2.2 IDS und IPS

Während die Firewall Pakete anhand von IP-Adressen und Ports filtert, untersucht das IDS/IPS den Inhalt auf bekannte Angriffsmuster (Signaturen). OPNsense nutzt hierfür die Open-Source-Engine Suricata, während Sophos auf eine eigene, auf Snort basierende Engine mit Sophos-Labs-Signaturen setzt („Sophos Endpoint IPS: Frequently asked questions“ o. J.; „Intrusion Prevention System — OPNsense documentation“ o. J.; Ltd o. J.-c; „Sophos UTM: Low throughput with Intrusion Prevention (IPS)“ o. J.).

Die IPS-Einstellungen findet man bei Sophos unter *Protect > Intrusion Prevention*. Sophos bietet vordefinierte Richtlinien und die Signaturen werden automatisch im Hintergrund aktualisiert.

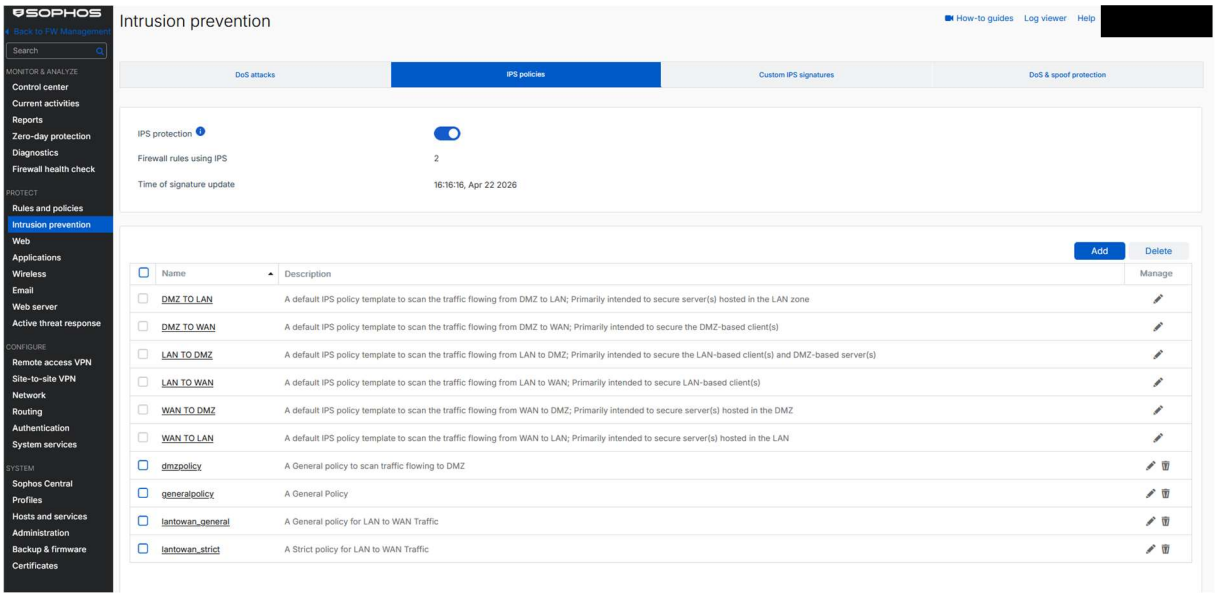


Abbildung 7: IPS Policies im Sophos Web-Admin

Die Konfiguration bei OPNsense befindet sich unter *Services > Intrusion Detection > Administration*.

1. Zunächst muss der Dienst aktiviert und an die gewünschten Schnittstellen (LAN/WAN) gebunden werden. Erst durch diese Konfiguration des „Capture mode“ wird die Umstellung von einem IDS zu einem aktiv eingreifenden IPS ermöglicht.

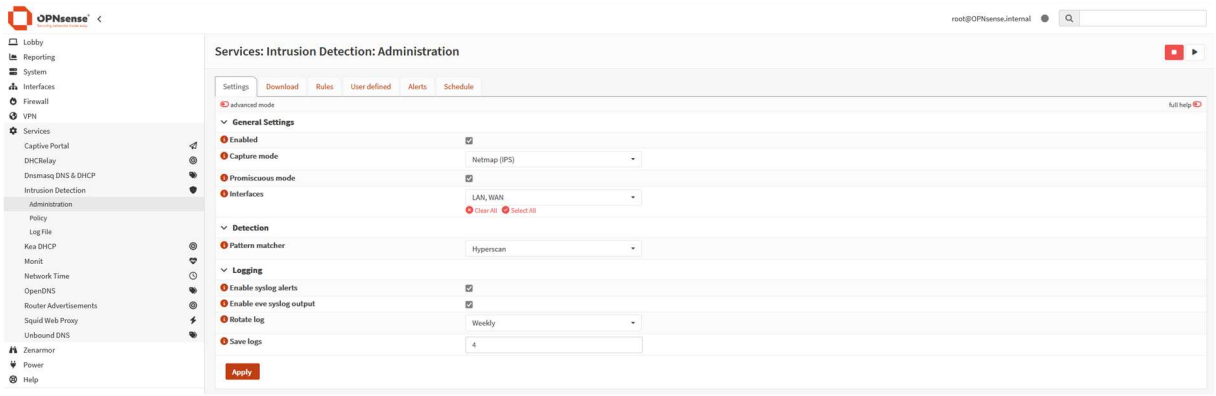


Abbildung 8: OPNsense IPS Administration

2. Innerhalb der Policy-Einstellungen lassen sich spezifische Regelsätze für das IPS konfigurieren und von externen Providern beziehen. Diese Regeln definieren die Kriterien, nach denen der Netzwerkverkehr analysiert und potenziell blockiert wird.

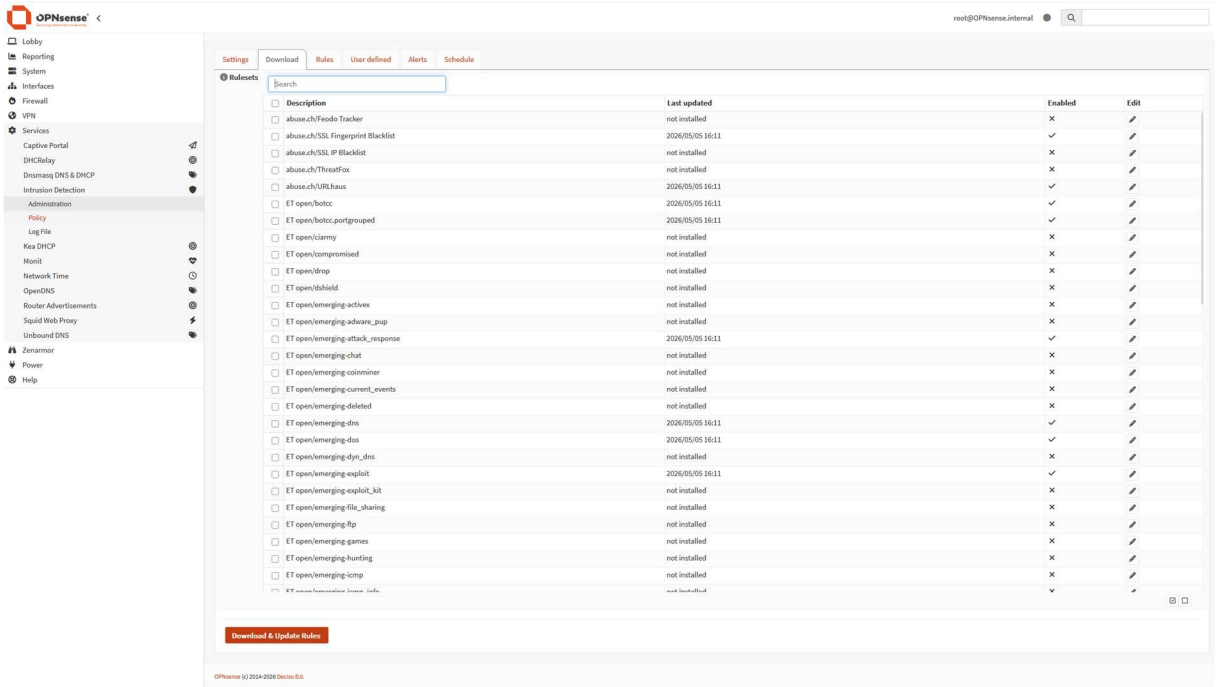
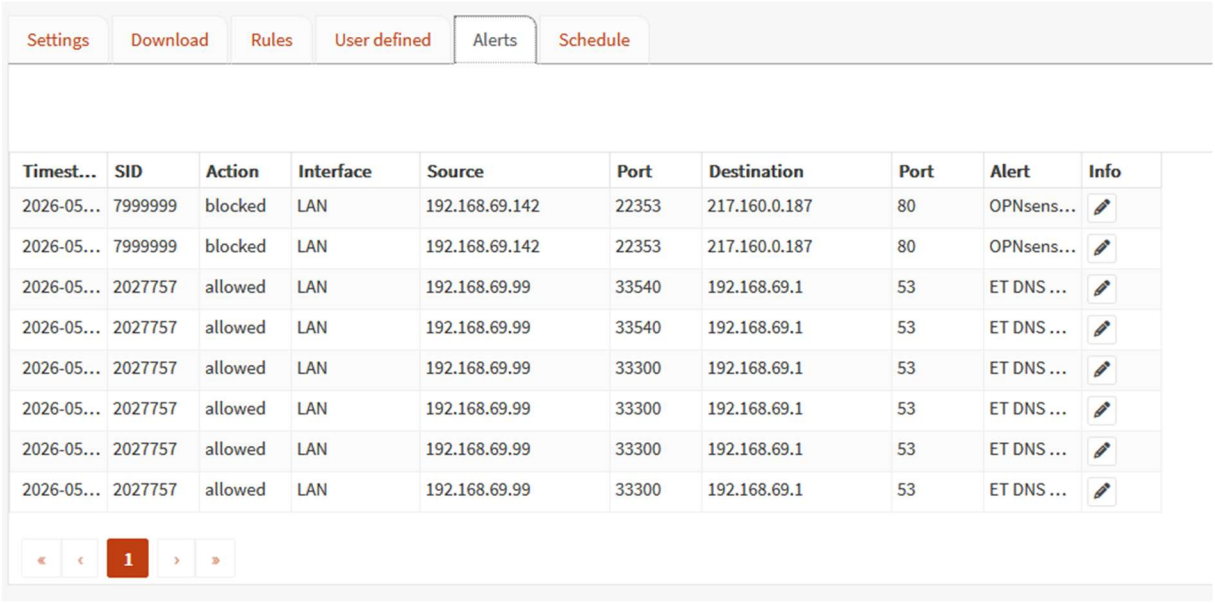


Abbildung 9:OPNsense IPS Regelwerk Download

Um die Funktionsfähigkeit des IPS zu bestätigen, wird versucht, die EICAR-Testdatei über eine unverschlüsselte HTTP-Verbindung zu laden. Die Firewall blockiert die Datei wie gewünscht („Download Anti Malware Testfile“ o. J.).

```
C:\Users\lucas>curl -X POST -d "X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*" http://testmyids.com
curl: (56) Recv failure: Connection was reset
```

Abbildung 10: Blockierter Curl Befehl mit EICAR- Testdatei



Timest...	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
2026-05...	7999999	blocked	LAN	192.168.69.142	22353	217.160.0.187	80	OPNsens...	
2026-05...	7999999	blocked	LAN	192.168.69.142	22353	217.160.0.187	80	OPNsens...	
2026-05...	2027757	allowed	LAN	192.168.69.99	33540	192.168.69.1	53	ET DNS ...	
2026-05...	2027757	allowed	LAN	192.168.69.99	33540	192.168.69.1	53	ET DNS ...	
2026-05...	2027757	allowed	LAN	192.168.69.99	33300	192.168.69.1	53	ET DNS ...	
2026-05...	2027757	allowed	LAN	192.168.69.99	33300	192.168.69.1	53	ET DNS ...	
2026-05...	2027757	allowed	LAN	192.168.69.99	33300	192.168.69.1	53	ET DNS ...	
2026-05...	2027757	allowed	LAN	192.168.69.99	33300	192.168.69.1	53	ET DNS ...	

Abbildung 11: OPNsense IPS blockiert EICAR- Testdatei

Die Sophos-Firewall detektierte und blockierte den entsprechenden Angriffsversuch ebenfalls unmittelbar und zuverlässig.

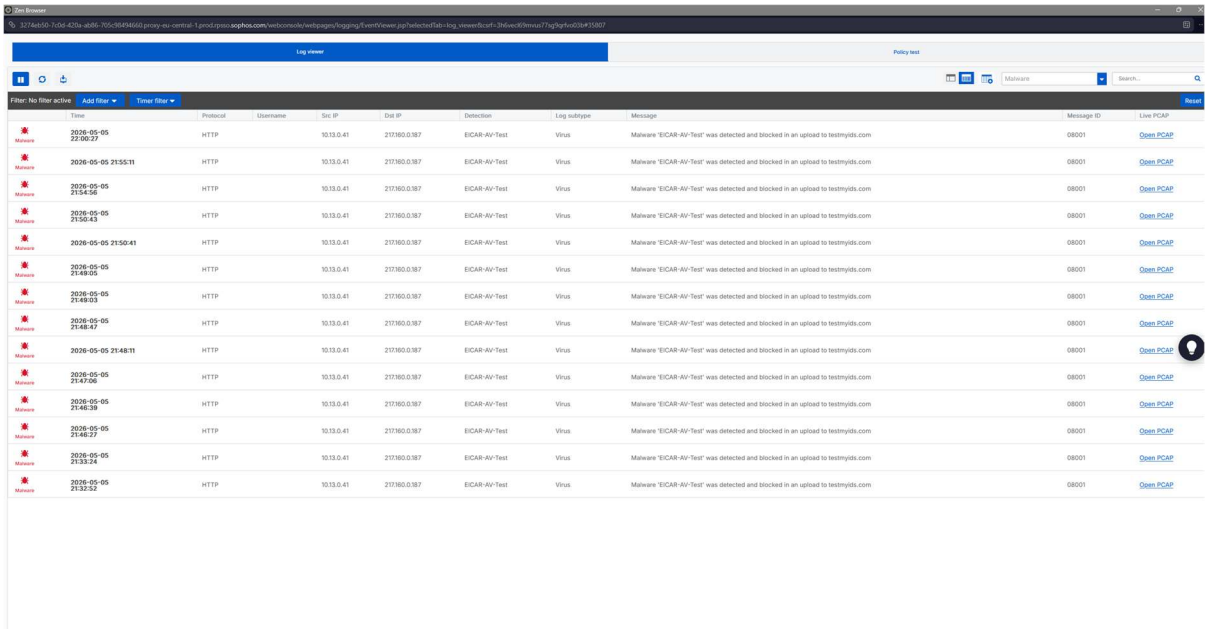


Abbildung 12: Sophos IPS blockiert EICAR- Testdatei

Sophos bietet ein Sorglos-Paket mit vorkonfigurierten Profilen. OPNsense bietet mit Suricata ein mächtiges Werkzeug, erfordert aber von den Administrierenden die manuelle Auswahl und Pflege der Regelsätze, um Fehlalarme zu vermeiden und die Blocklisten aktuell zu halten.

4.2.3 Webfilter

Der Webfilter dient der Kontrolle des Surfverhaltens und dem Schutz vor bösartigen Webseiten. Während klassische Firewalls nur auf IP-Basis blockieren, arbeitet der Webfilter auf Anwendungsebene (Layer 7). Er vergleicht aufgerufene URLs mit Kategorie Datenbanken und blockiert diese, wenn notwendig (z. B. Pornografie, Soziale Netzwerke, Malware).

Im nächsten Schritt werden die Mechanismen der „Web Protection“ einer vergleichenden Analyse unterzogen.

Sophos nutzt eine eigene, Cloud-basierte Datenbank. Die Konfiguration erfolgt über Web Policies, in denen ganze Kategorien (z. B. „Suspicious“ oder „Nudity and Adult Content“) per Mausklick gesperrt oder zeitlich begrenzt werden. Es können über sogenannte „Exceptions“ Ausnahmen definiert werden, die nicht gefiltert werden (z.B. O365). Um aktiviert zu sein, muss die Web Policy noch einer Regel hinzugefügt werden.

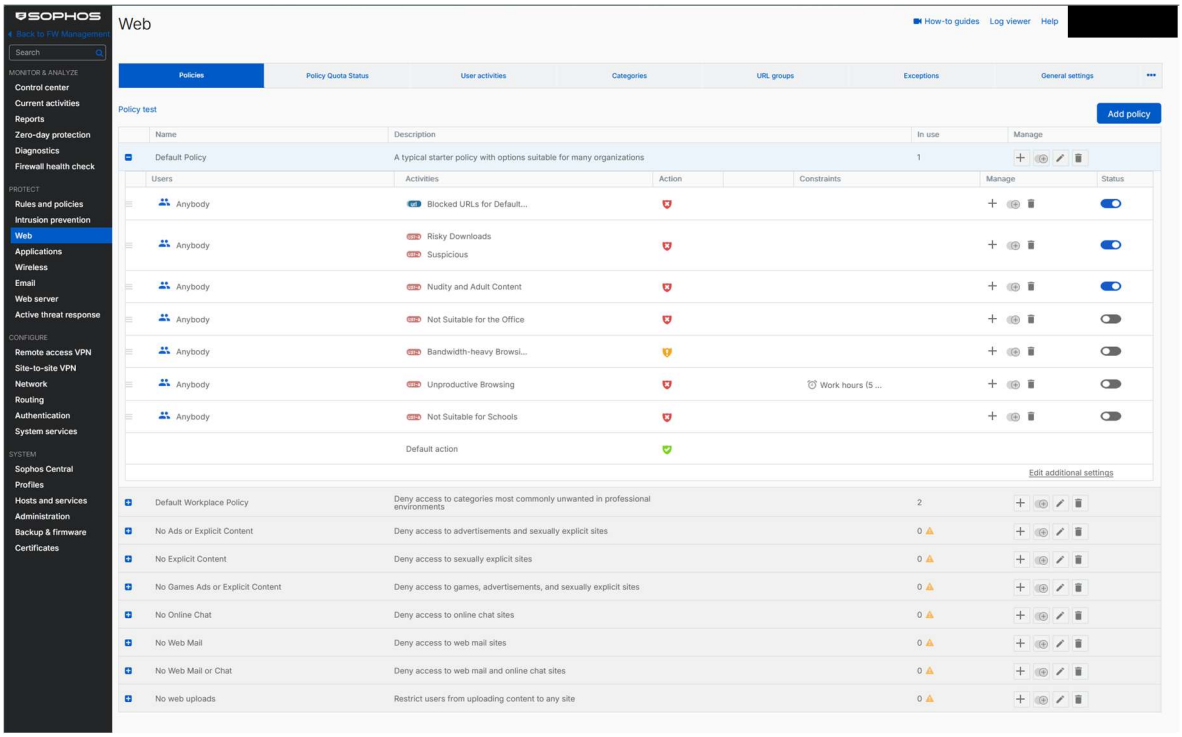


Abbildung 13: Kategorien-Übersicht in einer Sophos Web Policy

Die Implementierung der Web-Protection-Funktionalitäten wird unter OPNsense mithilfe des Plugins Zenarmor (ehemals Sensei) realisiert.

1. Hier ist die Installation des Plugins Zenarmor (os-sensei) zu sehen.

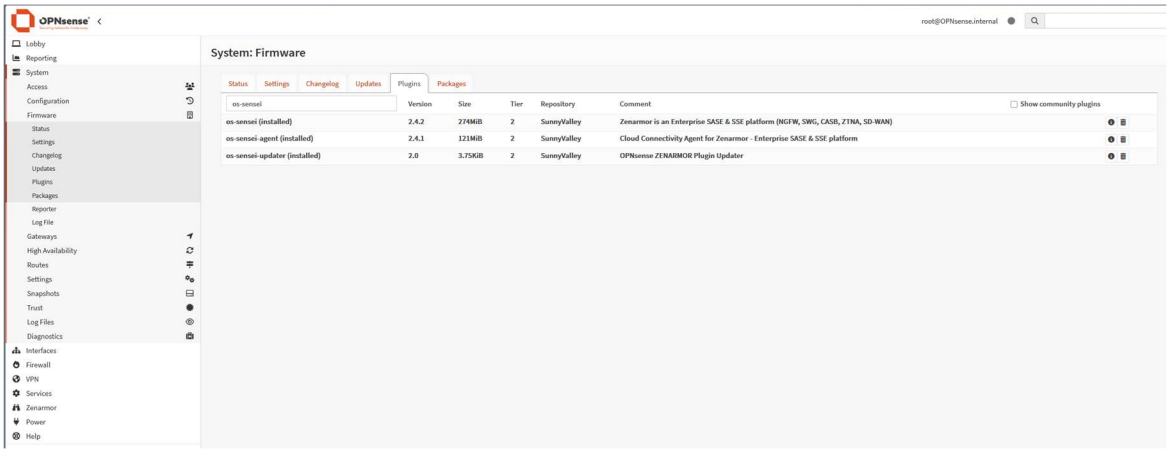


Abbildung 14: OPNsense installierte Plugins

2. Im zweiten Schritt folgt die Auswahl und Einrichtung der Datenbank zur Speicherung der Reporting- und Analysedaten. Hierbei kann zwischen einer lokalen Instanz und einer cloudbasierten Lösung gewählt werden.

3. Es folgt die Erstellung einer Richtlinie zur Inhaltsfilterung (z. B. die Sperrung der Kategorie „Gambling“). Es ist zu beachten, dass die kostenlose Edition funktionale Einschränkungen aufweist: Anstatt individuell konfigurierbarer Profile stehen hier lediglich vordefinierte Sicherheitsstufen wie „Permissive“, „Moderate“ oder „High Control“ zur Verfügung.

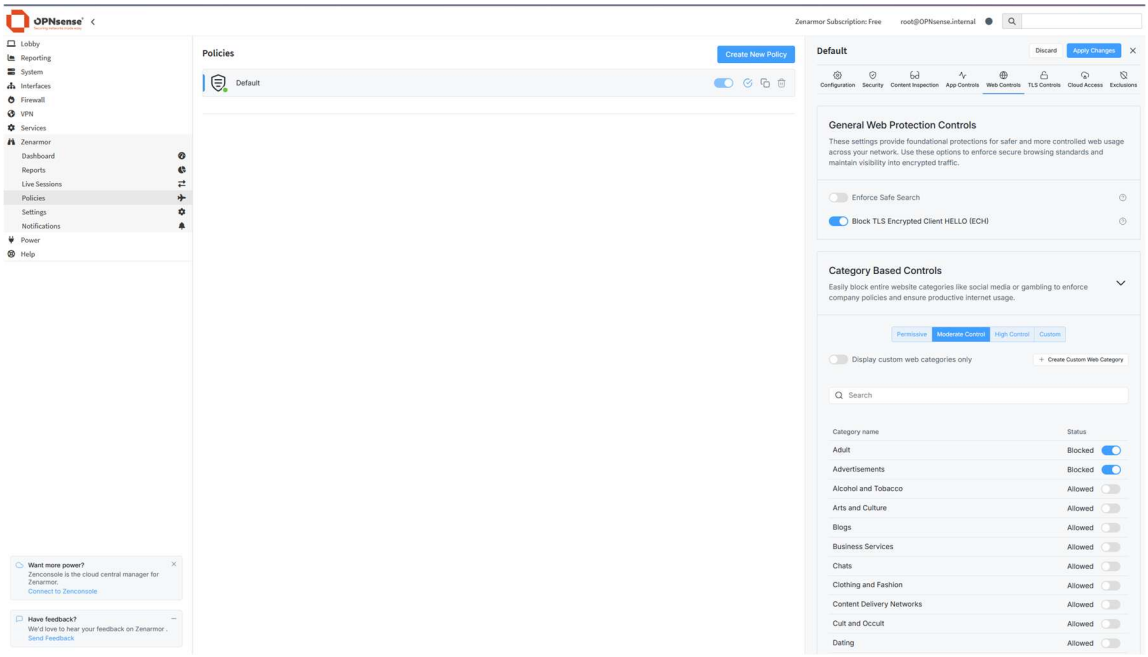


Abbildung 15: Die Zenarmor Policy-Konfiguration in OPNsense

Um die Funktion des Webfilters zu testen, wird eine Seite aufgerufen, die in die Kategorie Pornographie / Nudity fällt. Beide Firewalls haben für diesen Fall eine vordefinierte Kategorie, die ausgewählt werden kann.

Sowohl Zenarmor als auch Sophos blockieren die Seite zuverlässig.

OPNsense (Zenarmor) zeigt eine standardisierte Block-Seite.

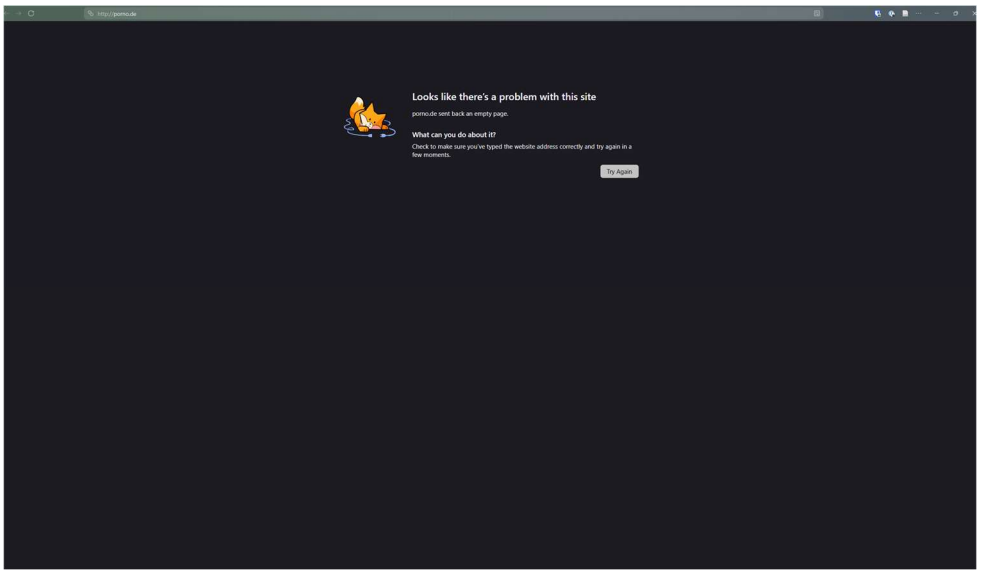


Abbildung 16: OPNsense blockierte Website

In den Log Files kann man erkennen, dass die Seite blockiert wird.

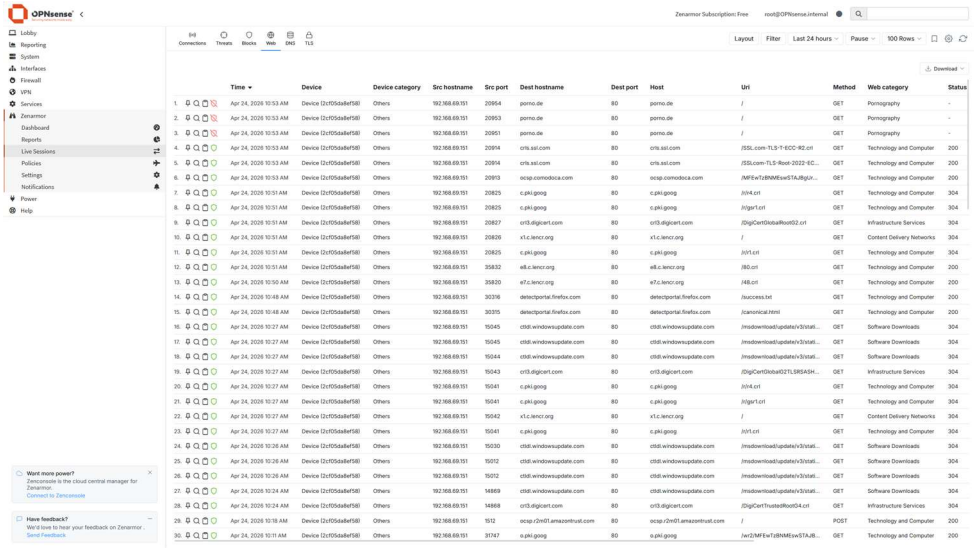


Abbildung 17: OPNsense Logs mit blockierter Website

Sophos bietet hier ein Corporate-Design mit Firmenlogo.

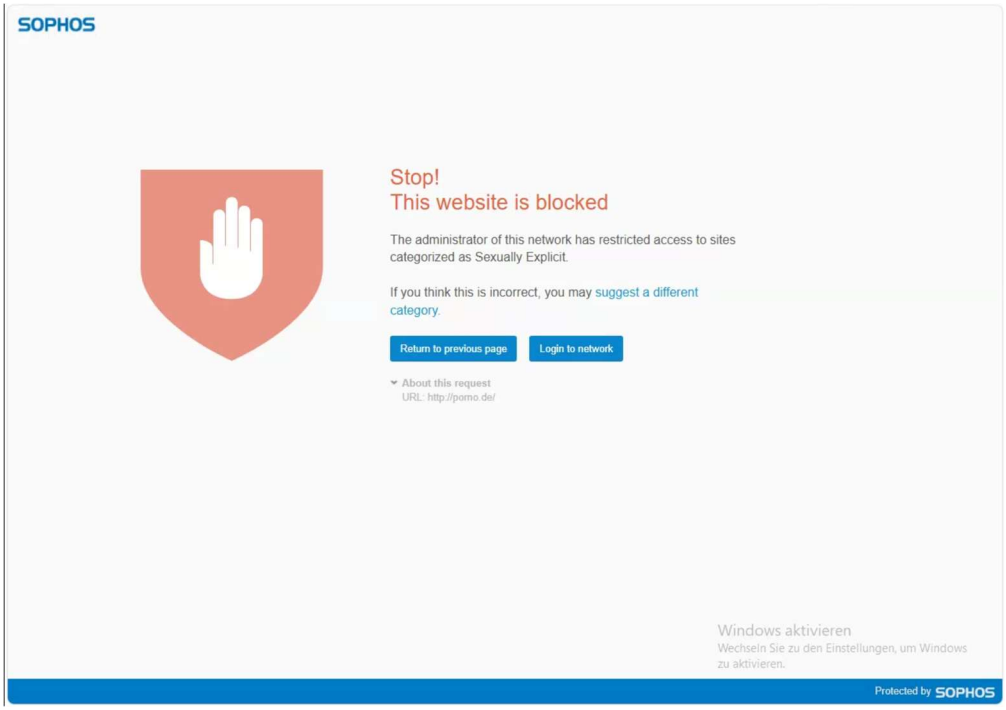


Abbildung 18: Sophos blockierte Website

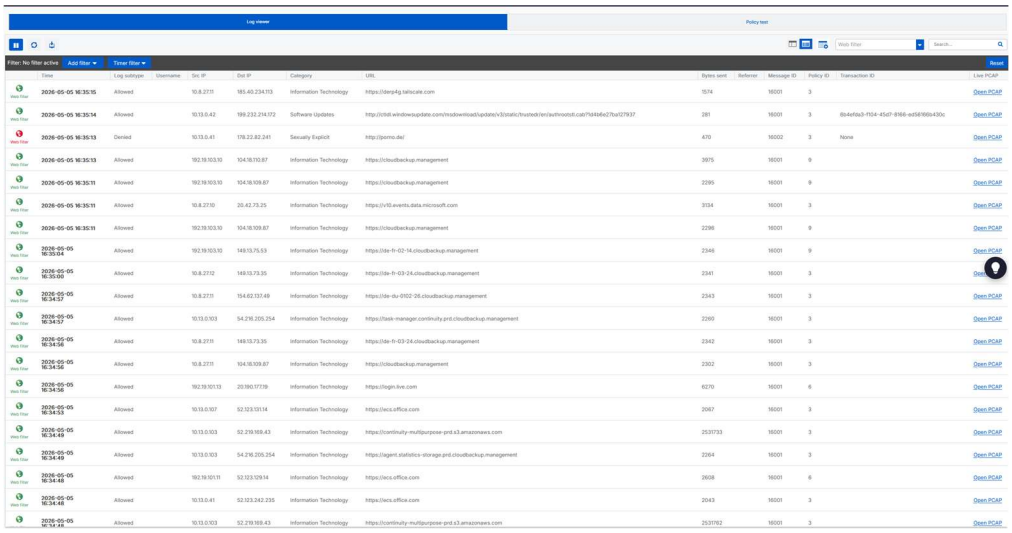


Abbildung 19: Sophos Logs mit blockierter Website

In der Standard-Installation bietet OPNsense nur einen rudimentären Proxy. Die geforderten Web-Control-Funktionalitäten lassen sich in OPNsense erst durch die Integration von Drittanbieter-Plugins, wie beispielsweise Zenarmor, annähernd realisieren. Dennoch bleiben in der kostenlosen Version einige Einschränkungen über Individualisierbarkeit des Webfilters. Sophos punktet hier durch die nahtlose Integration und die sehr feingliedrige Kategorisierung ab Werk. Gleichzeitig ist sie aber dennoch hochgradig personalisierbar.

4.2.4 Konnektivität

Die sichere Anbindung externer Beschäftigter ist eine Kernanforderung an moderne Firewalls. Hierbei steht nicht nur die Verschlüsselung im Vordergrund, sondern auch die Identitätsprüfung mittels MFA, um unbefugte Zugriffe durch gestohlene Zugangsdaten zu verhindern (BSI 2023, S. 739).

Im folgenden Abschnitt wird die praktische Anwendung der Remote-Access-Lösungen von Sophos untersucht.

Sophos bietet ein integriertes Self-Service-Portal, über das Beschäftigte VPN-Profile und den Client selbstständig beziehen können. MFA ist im System verwurzelt und kann einfach über den Sophos Authenticator oder Standard-Apps (Google/Microsoft) via QR-Code aktiviert werden. Es können ebenso Site-to-site VPNs konfiguriert werden, um zwei Netzwerke einfach zu verbinden.

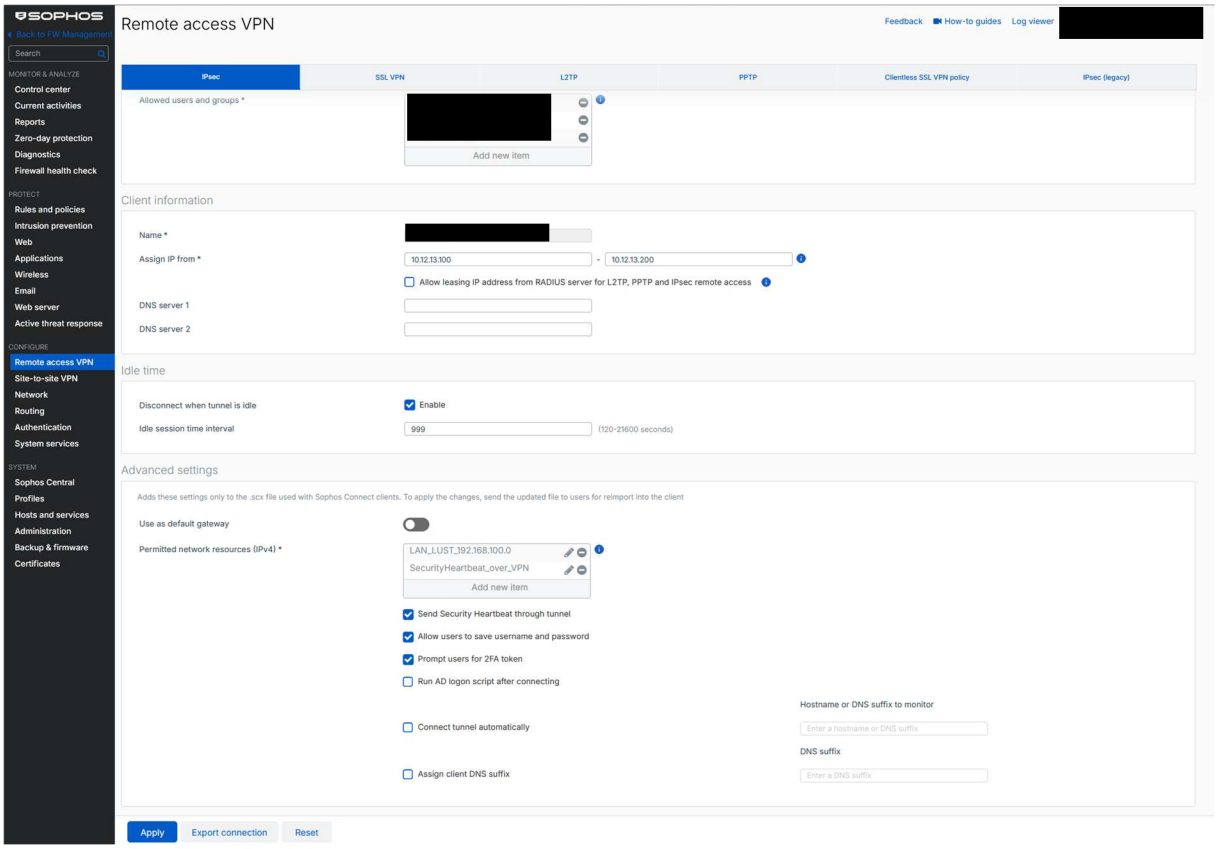


Abbildung 20: Sophos Remote access VPN IPsec

OPNsense bietet eine hohe Flexibilität bei der Bereitstellung von VPN-Diensten und unterstützt neben klassischen Protokollen wie IPsec und OpenVPN nativ das moderne und performante WireGuard. Ein zentraler Vorteil für die IT-Sicherheit ist die integrierte Unterstützung für die MFA, die beispielsweise über das TOTP-Verfahren direkt in den lokalen Authentisierungs-Server der Firewall eingebunden werden kann. Während diese Architektur die Sicherheit des Fernzugriffs massiv erhöht, ist der initiale Konfigurations- und Rollout-Aufwand im Vergleich zu proprietären Systemen höher einzustufen. Da OPNsense über kein automatisiertes Self-Service-Portal für Endanwendende verfügt, müssen VPN-Profile und Zertifikate manuell generiert und sicher an die Mitarbeitenden übermittelt werden. Der administrative Aufwand verschiebt sich hierbei von Lizenzkosten hin zu einer intensiveren Betreuung durch das IT-Dienstleistungsunternehmen.

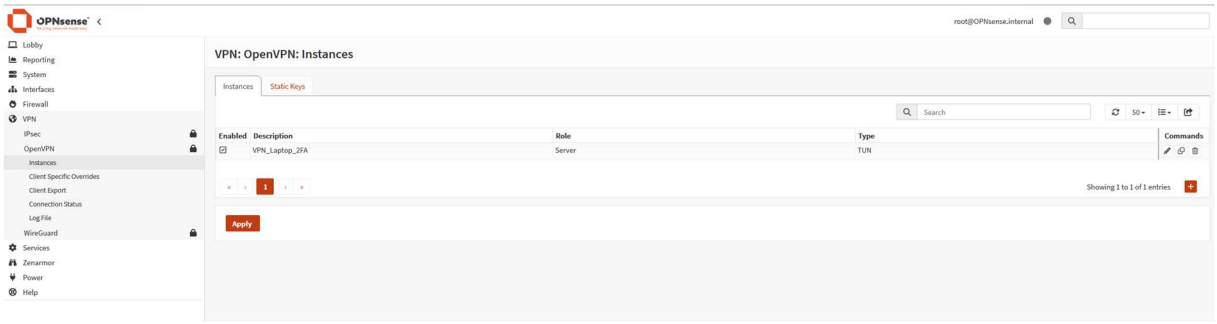


Abbildung 21: OpenVPN und weitere VPNs in OPNsense

In der Hinsicht auf die möglichen VPN-Technologien stehen sich die beiden Systeme in nichts nach. Sophos gewinnt jedoch beim Life-Cycle-Management: Das automatisierte Portal spart signifikant Zeit und Konfigurations-Aufwand. OPNsense unterstützt modernste Protokolle wie WireGuard, der Aufwand in der Einrichtung ist aber deutlich höher als bei Sophos.

4.3 Administration und Incident-Management

Die Effektivität einer Firewall hängt maßgeblich davon ab, wie effizient sich Administrierende Informationen extrahieren können. Um in der Praxis Angriffe gezielt zu erkennen, muss die Benutzeroberfläche Bedrohungen priorisiert darstellen und eine schnelle Ursachenanalyse ermöglichen (BSI 2023, S. 734).

4.3.1 Dashboard-Visualisierung und Alerting

Das klassische Dashboard nennt Sophos „Control Center“. Sophos nutzt ein Ampelsystem. Das Dashboard zeigt sofort den „Security Heartbeat“ (Zustand der Endgeräte) und kritische Angriffe in Signalfarben. Benachrichtigungen (Alerting) können direkt per E-Mail oder über das Central-Portal konfiguriert werden. Dieses ist unter *System services > Notification List* zu finden.

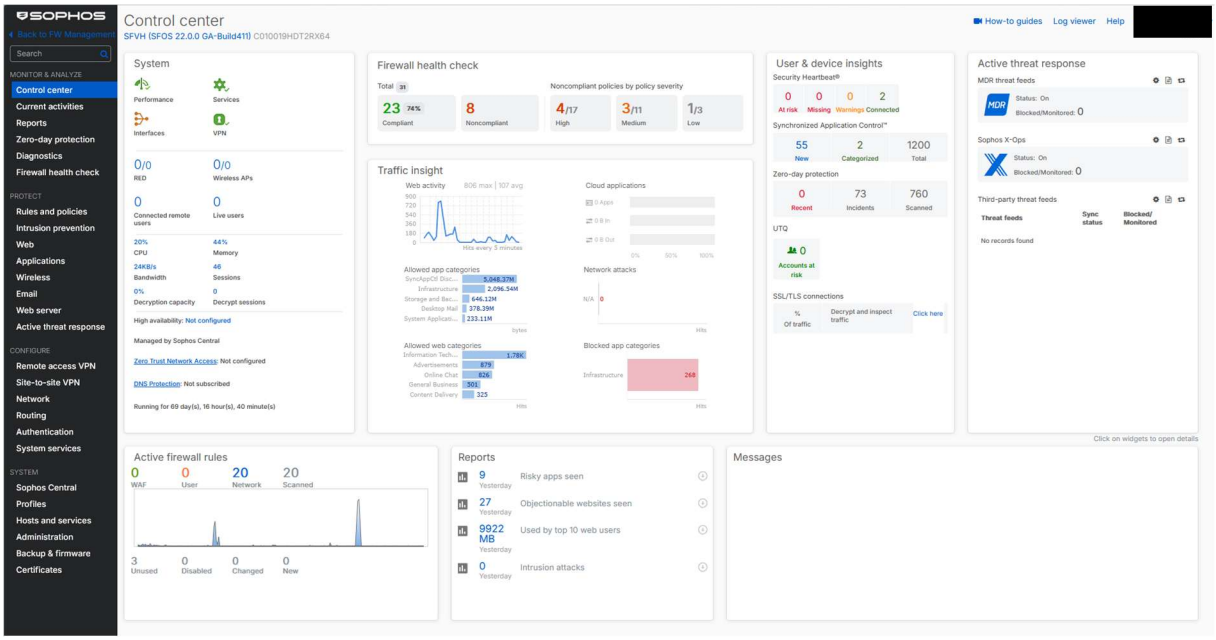


Abbildung 22: Sophos Dashboard bei einem KMU

Das Dashboard von OPNsense folgt einem modularen Konzept. Während die Standardkonfiguration primär systemrelevante Parameter wie CPU-Auslastung und Arbeitsspeichernutzung visualisiert, erfordert die Darstellung sicherheitsrelevanter Daten eine manuelle Anpassung. Informationen zu Ereignissen des IPS (Suricata) oder des Webfilters (Zenarmor) müssen über spezifische Widgets hinzugefügt werden. Ergänzend dazu lässt sich unter *Services > Monit* ein Alerting für definierte Systemereignisse konfigurieren.

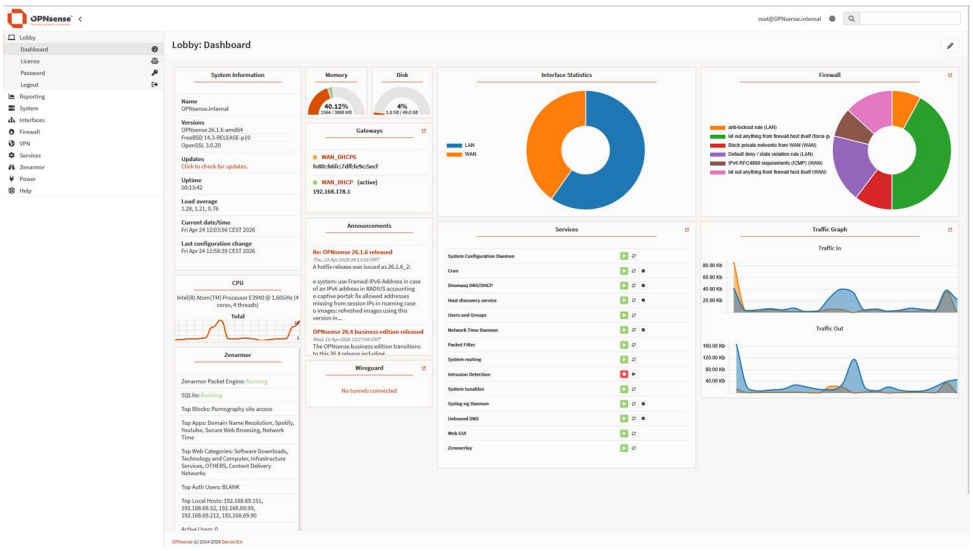


Abbildung 23: OPNsense Dashboard mit Plugin Widgets

Obwohl beide Systeme Dashboards sowie Alerting- und Monitoring-Funktionen bieten, die individuell vom Administrierenden konfiguriert werden können, überzeugt das Sophos Control Center durch eine höhere Aussagekraft. Es liefert mehr relevante Informationen auf einen Blick und ist in der Handhabung deutlich einfacher und intuitiver gestaltet.

4.3.2 Logging-Tiefe und Monitoring

Sophos bietet einen interaktiven Log Viewer, der Logs nach Funktionsbereichen (Webfilter, Firewall, IPS) trennt. Der Log Viewer von Sophos ist oben rechts in der Sophos Admin Console zu finden. Die Lösung umfasst einen Policy-Test zur Überprüfung von Richtlinien durch den Administrierenden. Ergänzend dazu besticht der Log Viewer durch seine übersichtliche Struktur sowie umfangreiche Filteroptionen, die eine detaillierte Informationsanalyse ermöglichen.

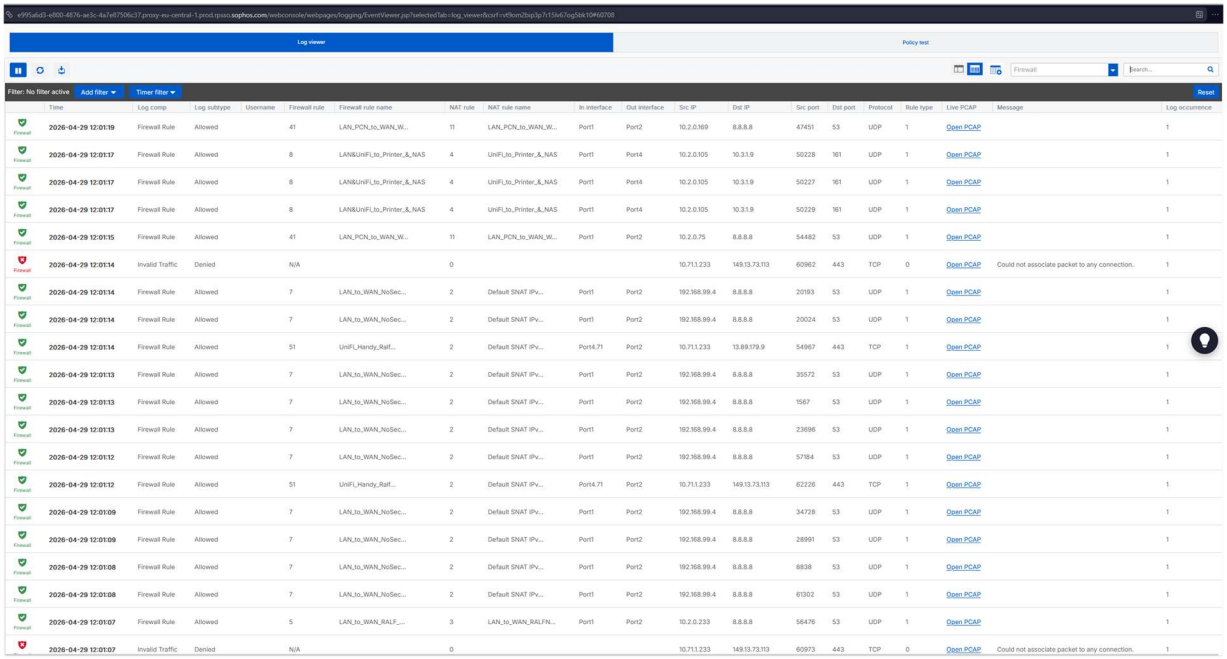


Abbildung 24: Der Log Viewer von Sophos

OPNsense bietet sehr tiefe, technisch detaillierte Echtzeit-Logs. Die Firewall Logs sind bei OPNsense unter *Firewall > Log Files > Live View* zu finden. Diese sind jedoch weniger aufbereitet und unübersichtlicher dargestellt. Für eine grafische Aufarbeitung ist die Nutzung von Plugins wie Zenarmor oder die Anbindung an externe Systeme (z. B. InfluxDB/Grafana) nötig.

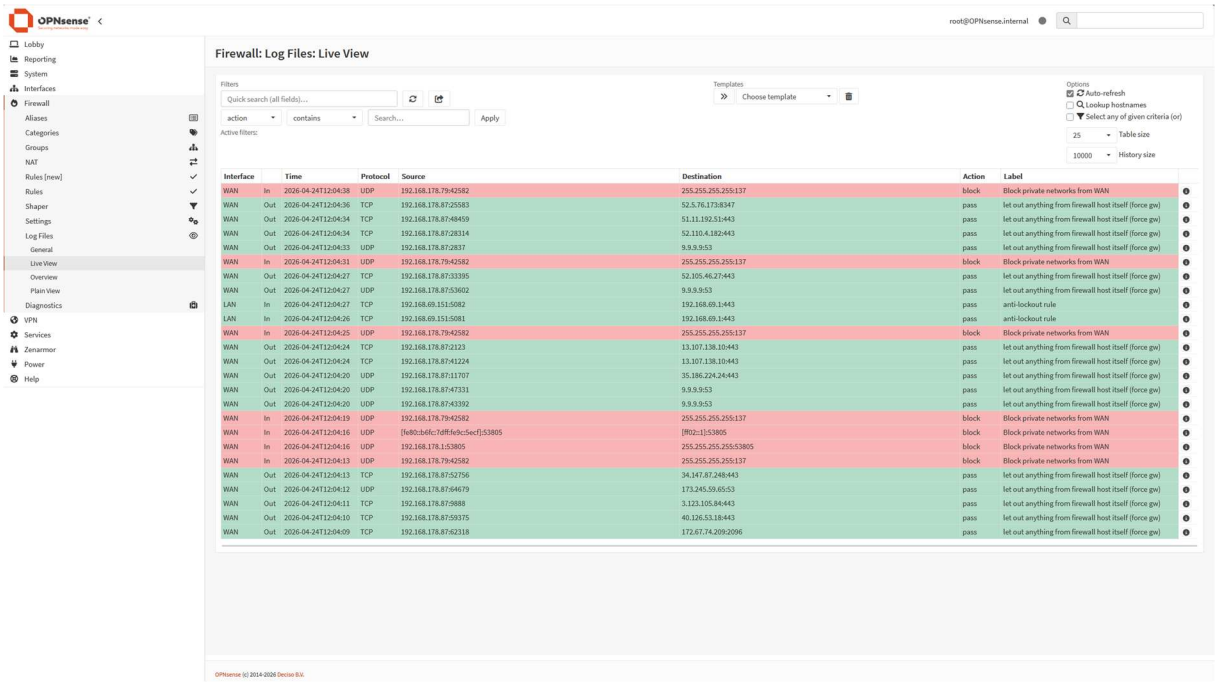


Abbildung 25: Die Live-View-Ansicht der OPNsense Firewall

Während die Sophos XGS auf „Management by Exception“ optimiert ist (die Sophos meldet sich nur, wenn etwas nicht stimmt), ist OPNsense ein mächtiges Diagnose-Werkzeug, das jedoch mehr Aufmerksamkeit und Fachwissen vom Administrierenden verlangt, um aus den angezeigten Informationen die relevanten Incidents herauszufiltern.

4.4 Wartbarkeit und Supply-Chain-Sicherheit

Die Sicherheit einer Firewall ist kein statischer Zustand, sondern ein kontinuierlicher Prozess. Da ständig neue Bedrohungen identifiziert werden, ist die Reaktionsgeschwindigkeit der Entwickler auf bekannt gewordene Schwachstellen (CVEs) ein entscheidendes Qualitätsmerkmal für die digitale Resilienz eines KMU.

4.4.1 Patch-Management und Reaktionszeiten

Sophos agiert als kommerzieller Hersteller mit festen Release-Zyklen für die Firmware der XGS-Serie. Patches für kritische Lücken werden oft zeitnah als "Hotfixes" ausgerollt, die ohne kompletten Neustart eingespielt werden können. Das Administrationspersonal ist von der Priorisierung des Herstellers abhängig. Proprietärer Code (Closed Source) macht es unmöglich, die Korrektheit des Patches unabhängig zu prüfen.

Die Update-Historie der OPNsense ist unter *System > Firmware > Status* zu finden.

OPNsense zeichnet sich durch eine sehr hohe Update-Frequenz aus (alle zwei Wochen ein Minor Release). Kritische Sicherheitslücken werden oft innerhalb weniger Stunden nach Bekanntwerden durch die Community oder den Sponsor Deciso geschlossen. Ein konkreter Beleg für diese Reaktionsschnelligkeit ist das Release 24.7.1: Nachdem das FreeBSD-Projekt am 07. August 2024 mehrere kritische Sicherheitsmeldungen (Security Advisories) veröffentlicht hatte, stellte OPNsense bereits am Folgetag, den 08. August 2024, ein vollständiges Sicherheitsupdate bereit. In den offiziellen Release Notes wird explizit auf die Schließung dieser Sicherheitslücken innerhalb von weniger als 24 Stunden verwiesen („FreeBSD 14.1-RELEASE Errata“ o. J.; „OPNsense 24.7.1 released“ o. J.). Diese hohe Patch-Frequenz ist insbesondere für KMU von Bedeutung, da sie das Zeitfenster für potenzielle Angriffe auf kritische Infrastrukturen minimiert.

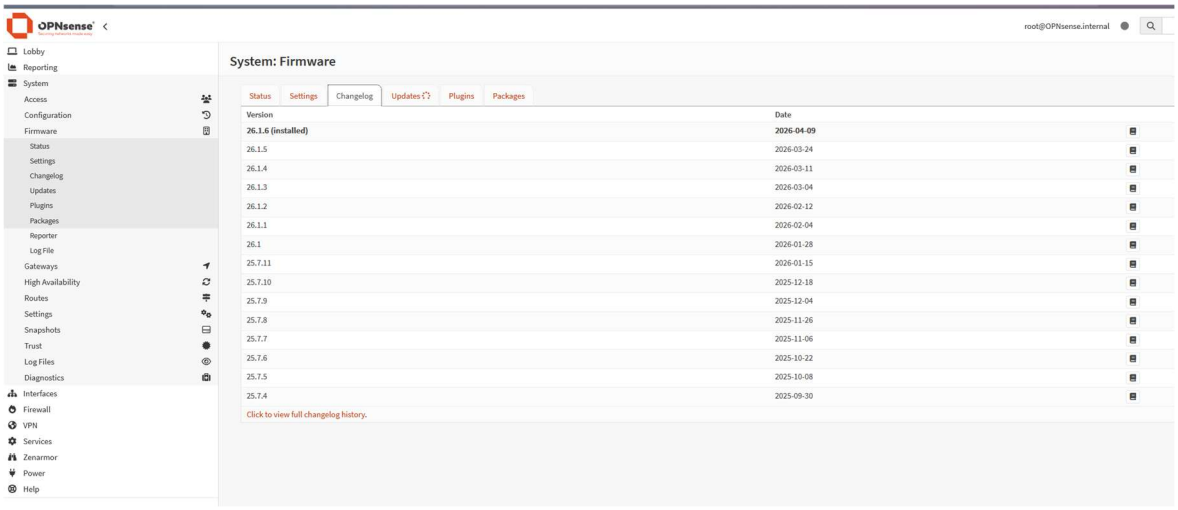


Abbildung 26: Die Change-Log-Historie in der OPNsense-GUI

4.4.2 Supply-Chain-Transparenz

Sophos ist ein globales Unternehmen mit Sitz in Großbritannien und im Besitz durch US-Investoren. Die Lieferkette ist hochgradig optimiert, aber durch den proprietären Ansatz nicht vollständig Transparent gestaltet („Cybersecurity as a Service Delivered“ o. J.).

OPNsense basiert auf HardenedBSD, einem sicherheitsoptimierten Ableger von FreeBSD. Der gesamte Quellcode ist auf GitHub öffentlich einsehbar, also vollständig Open Source („OPNsense“ o. J.).

Die Kombination aus der LINCE-Zertifizierung der Business-Lizenz und der Verwendung moderner MVC-Frameworks gewährleistet eine transparente Code-Basis. Die Transparenz des Quellcodes ermöglicht eine kontinuierliche Prüfung durch die globale Community. Durch dieses Prinzip der kollektiven Kontrolle wird das Risiko für unentdeckte Schwachstellen oder absichtliche Manipulationsversuche (Backdoors) signifikant minimiert, da jede Code-Änderung öffentlich nachvollziehbar ist („The cathedral and the bazaar: musings on Linux and open source by an accidental revolutionary“ 2002, S. 30).

OPNsense bietet durch die Offenlegung des Quellcodes und die agilen Update-Zyklen eine sehr hohe Supply-Chain-Sicherheit. Sophos punktet hingegen mit einer strukturierten Patch-Policy, die für das Administrationspersonal oft weniger Eigeninitiative (wie das tägliche Lesen von Foren) erfordert.

5. Wirtschaftlichkeitsanalyse

Neben der technischen Leistungsfähigkeit ist die ökonomische Effizienz ein ausschlaggebendes Kriterium für die Auswahl einer Sicherheitslösung im KMU-Umfeld. IT-Entscheidungen werden heute zunehmend unter dem Aspekt der strategischen Kostenoptimierung getroffen, wobei nicht nur die unmittelbaren Anschaffungskosten, sondern die gesamte wirtschaftliche Belastung über den Lebenszyklus einer Lösung betrachtet werden müssen.

Ziel dieses Kapitels ist es, die OPNsense-Software und die Sophos XGS-Plattform hinsichtlich ihrer finanziellen Auswirkungen gegenüberzustellen. Hierzu wird im ersten Schritt das Modell der Total Cost of Ownership (TCO) angewandt, um eine ganzheitliche Kostenübersicht über einen Betrachtungszeitraum von drei Jahren zu erstellen. Dabei werden neben den Investitionskosten (CAPEX) auch die laufenden Betriebskosten (OPEX), wie Lizenzgebühren und administrativer Aufwand, berücksichtigt.

Anschließend folgt ein direkter Vergleich der Lizenzmodelle, gefolgt von einer kritischen Auseinandersetzung mit den Themen Haftung und SLA. Diese Analyse dient als betriebswirtschaftliche Entscheidungsgrundlage, um zu bewerten, ob die Kostenvorteile einer Open-Source-Lösung die potenziellen Mehraufwände in der Eigenverwaltung und Risikoabsicherung rechtfertigen. Die folgende Wirtschaftlichkeitsbetrachtung erfolgt mittels eines gängigen Vergleichs der TCO in Anlehnung an betriebswirtschaftliche Standardverfahren.

5.1 TCO über 3 Jahre

Die TCO (Gesamtkosten des Betriebs) ist ein betriebswirtschaftliches Rechenmodell, das darauf abzielt, alle anfallenden Kosten einer Investition offenzulegen. Für ein KMU ist nicht nur der Anschaffungspreis entscheidend, sondern vor allem die laufenden Kosten für Wartung, Lizenzen und Energie über den gesamten Lebenszyklus der Hardware. In dieser Arbeit wird ein Betrachtungszeitraum von drei Jahren gewählt, was dem üblichen Abschreibungs- und Supportzyklus für Netzwerk-Hardware entspricht.

5.1.1 Kalkulationsparameter und Annahmen

Um einen gerechten Vergleich zwischen der OPNsense im Labor-Umfeld und der Sophos XGS im Kunden-Umfeld zu ermöglichen, werden folgende Rahmenbedingungen für ein Muster-KMU (ca. 30–50 Mitarbeiter) definiert:

- Personalkosten: Für administrative Tätigkeiten wird ein kalkulatorischer Stundensatz von 80,00 € angesetzt (brutto inkl. Lohnnebenkosten).
- Wartungsaufwand:
    - Für die Sophos XGS wird ein Aufwand von 1 Stunde/Monat kalkuliert (höherer Automatisierungsgrad).
    - Für die OPNsense wird ein Aufwand von 2 Stunden/Monat kalkuliert (manuelle Prüfung der Community-Updates, Feinjustierung der Open-Source-Regelwerke).
- Betriebszeit: Sind bei beiden Geräten identisch. Die Stromkosten werden in dieser TCO nicht berücksichtigt.

5.1.2 Investitionskosten (CAPEX)

Die Capital Expenditures (CAPEX) umfassen die einmaligen Kosten zu Beginn des Projekts.

Position	**Sophos XGS 118**	**OPNsense DEC740**
Hardware-Anschaffung	ca. 735,00 €	ca. 878,00 €
Initiales Setup & Konfiguration	4 Std. (320,00 €)	8 Std. (640,00 €)
Summe CAPEX	**1.055,00 €**	**1.518,00 €**

Tabelle 3: CAPEX Kostenvergleich Sophos und OPNsense

(GmbH o. J.-b; „DEC740 – OPNsense® Desktop Security Appliance“ o. J.)

Bei den Anschaffungskosten zeigt sich, dass die OPNsense-Lösung (basierend auf Deciso-Hardware) in der reinen Anschaffung kostspieliger ist als die Sophos XGS 118. Berücksichtigt man zudem den erhöhten manuellen Konfigurationsaufwand für die modulare Einrichtung von OPNsense, ergibt sich eine finale Kostendifferenz von 463,00 € zulasten der Open-Source-Lösung. Dieser Mehrwert bei Sophos resultiert primär aus einer höheren Out-of-the-Box-Effizienz und einem geringeren Implementierungsaufwand pro Arbeitsstunde. Die Anschaffungskosten der OPNsense-Lösung lassen sich signifikant reduzieren, indem anstelle dedizierter Deciso-Appliances eine Eigenbau-Hardware verwendet wird.

5.1.3 Betriebskosten (OPEX)

Die Operational Expenditures (OPEX) bilden die laufenden Kosten über 36 Monate ab.

Position	**Sophos XGS (3J. Xstream)**	**OPNsense (Business Edition)**
Lizenzgebühren	ca. 3.390,00 €	ca. 300,00 €
Administrative Wartung (36 Monate)	36 Std. (2.880,00 €)	72 Std. (5.760,00 €)
Summe OPEX	**6.270,00 €**	**6.060,00 €**

Tabelle 4: OPEX-Kostenvergleich Sophos und OPNsense

(„OPNsense® Business Edition 1yr subscription“ o. J.; GmbH o. J.-a)

Während die Lizenzkosten bei der OPNsense deutlich geringer ausfallen, gleicht sich der Gesamtpreis durch die höheren Wartungskosten wieder aus.

5.1.4 Zusammenfassung der TCO

Die Wirtschaftlichkeitsanalyse verdeutlicht, dass die Wahl einer Sicherheitslösung im KMU-Umfeld über die reinen Anschaffungskosten hinaus eine ganzheitliche Betrachtung der TCO erfordert. Im direkten Vergleich verursacht die Sophos XGS 118 geringere Investitionskosten (CAPEX). Zwar ist die OPNsense-Hardware teurer, doch entscheidend ist der Zeitaufwand: Die effiziente Ersteinrichtung der Sophos-Lösung gleicht den höheren Anschaffungspreis und die zeitintensive Konfiguration der OPNsense mehr als aus. Es muss beachtet werden, dass bei der DEC740 die OPNsense Business Edition bereits 1 Jahr inkludiert ist. Aufgrund dessen wurde bei der OPEX die Business Edition Lizenz Kosten dementsprechend angepasst.

In der Betriebsphase (OPEX) kehrt sich dieses Verhältnis zwar aufgrund der geringen Lizenzgebühren der OPNsense Business Edition um, allerdings wird dieser finanzielle Vorteil nahezu vollständig durch den doppelten administrativen Wartungsaufwand der Open-Source-Lösung neutralisiert. In der Gesamtkalkulation über drei Jahre erweisen sich beide Systeme als nahezu kostenneutral zueinander. Somit stellt nicht der Preis, sondern die Abwägung zwischen hohen Lizenzkosten bei Sophos gegenüber einem gesteigerten personellen Eigenaufwand bei OPNsense das zentrale betriebswirtschaftliche Entscheidungskriterium dar.

5.2 Lizenzmodelle und Subscriptions

Ein wesentlicher Unterschied liegt in der Ausgestaltung der Lizenzen der beiden Anbieter:

Sophos Xstream Protection: Nach Ablauf der Lizenz werden alle Sicherheitsfeatures wie der Webfilter oder das IPS deaktiviert. Die Firewall sinkt auf das Niveau eines einfachen Routers herab (Ltd o. J.-a).

OPNsense Business Edition: Die Lizenzkosten decken hier primär den professionellen Support, kommerzielle Rule-Sets und die Stabilität der Firmware ab. Sollte die Lizenz nicht verlängert werden, bleiben alle Funktionen der Firewall (inkl. IPS/Webfilter) funktionsfähig. Um zusätzliche Support-Leistungen zu erhalten, müssen zusätzliche Support Stunden erworben werden („Product categories Support“ o. J.-b; „OPNsense® Business Edition 1yr subscription“ o. J.).

5.3 Haftung & SLA

Ein oft unterschätzter Aspekt beim Vergleich von Open-Source-Software und proprietären Lösungen ist die vertragliche Absicherung im Ernstfall. Während die technischen Funktionen (siehe Kapitel 4) nahezu identisch sein können, unterscheiden sich die Verantwortlichkeiten und Support-Strukturen erheblich.

5.3.1 Hersteller-Support vs. Eigenverantwortung

Bei der Sophos XGS ist der Support fester Bestandteil des Lizenzmodells. Das „Enhanced Support“-Paket garantiert dem KMU definierte Reaktionszeiten und einen direkten Ansprechpartner beim Hersteller. Im Falle eines Hardware-Defekts wird durch das „Advance Replacement“ sichergestellt, dass Ersatzhardware oft bereits am nächsten Werktag eintrifft. Diese Kosten sind in den hohen Lizenzgebühren (siehe Kapitel 5.1.3) bereits enthalten (Ltd o. J.-b).

Bei OPNsense basiert der Support primär auf der Community und einer umfangreichen Dokumentation. Die in dieser Arbeit betrachtete Business Edition bietet zwar eine höhere Stabilität durch geprüfte Updates, beinhaltet jedoch keinen individuellen Support mit garantierten Reaktionszeiten (SLA). Die Dienstleistenden trägt hier das Risiko von Ausfallzeiten selbst, sofern keine zusätzlichen Vorkehrungen getroffen werden.

5.3.2 Strategische Reinvestition der Lizenzersparnis

Die massive Ersparnis bei den Lizenzkosten (ca. 3090,00 € über 3 Jahre) sollte nicht als reine Gewinnmaximierung betrachtet werden, sondern ermöglicht eine strategische Umschichtung des Budgets. Da beim Einsatz von Open-Source-Software die direkte Herstellerhaftung entfällt, übernehmen die IT-Dienstleistungsunternehmen die Verantwortung für die Betriebssicherheit. Die freiwerdenden Mittel werden gezielt in die Service-Qualität reinvestiert:

SLA durch das Dienstleistungsunternehmen: Anstatt Lizenzgebühren an einen globalen Konzern wie Sophos abzuführen, investiert das KMU in ein lokales SLA. Das Dienstleistungsunternehmen garantiert hierbei spezifische Reaktionszeiten und übernimmt das kontinuierliche Patch-Management sowie die Überwachung der Firewall. Dies stellt sicher, dass die rechtlichen Anforderungen an die Sorgfaltspflicht erfüllt werden. Das bedeutet aber auch, dass das Dienstleistungsunternehmen die Verantwortung nicht auslagern kann.

Redundanz und Hardware-Management: Da bei Eigenbau-Hardware kein "Advance Replacement" durch einen Hersteller existiert, nutzt das Dienstleistungsunternehmen einen Teil der Budgetersparnis, um eine Hardware-Redundanz zu schaffen. Dies kann durch die Vorhaltung von vorkonfigurierten Ersatzgeräten (Cold Standby) oder den Aufbau eines Hochverfügbarkeits-Clusters erfolgen, um einen SPoF zu vermeiden.

5.3.3 Haftung und Professionalisierung

Während Sophos den Support als inkludiertes Produktmerkmal führt, wird bei der OPNsense-Lösung das Dienstleistungsunternehmen zum zentralen Haftungsanker. Dies erfordert eine Professionalisierung der Service-Prozesse: Das Dienstleistungsunternehmen muss durch regelmäßige Wartungsintervalle und ein lückenloses Monitoring sicherstellen, dass das Sicherheitsniveau dem "Stand der Technik" entspricht. Das KMU profitiert hierbei von einer persönlichen Betreuung und einer Firewall, die exakt auf die betrieblichen Anforderungen zugeschnitten ist, anstatt ein standardisiertes, aber teures Lizenzpaket zu finanzieren.

6. Zusammenfassung und Ausblick

In diesem letzten Kapitel werden die im Rahmen dieser Arbeit gewonnenen technischen und wirtschaftlichen Erkenntnisse zusammengeführt, um ein abschließendes Urteil über die Eignung der OPNsense als Alternative zur Sophos XGS im KMU-Umfeld zu fällen. Basierend auf dem direkten Vergleich der Sicherheitsfeatures und der TCO werden die eingangs formulierten Forschungsfragen beantwortet und ein Ausblick auf zukünftige Entwicklungen im Bereich der Open-Source-Netzwerksicherheit gegeben.

6.1 Zusammenfassung der Ergebnisse

Die im Rahmen dieser Bachelorarbeit durchgeführte Untersuchung liefert ein klares Bild über die Eignung von Open-Source-Firewalls für den KMU-Sektor. Die Ergebnisse lassen sich in die Bereiche technische Leistungsfähigkeit, administrative Effizienz und wirtschaftliche Attraktivität unterteilen:

Technische Leistungsfähigkeit: Der Praxisvergleich hat bestätigt, dass OPNsense technisch auf Augenhöhe mit etablierten proprietären Lösungen wie der Sophos XGS agiert. Wesentliche Sicherheitsmerkmale wie DPI, IDS/IPS, Webfilterung und moderne VPN-Protokolle wie OpenVPN und WireGuard lassen sich in OPNsense stabil realisieren. Voraussetzung für diesen Funktionsumfang ist jedoch die gezielte Nutzung von Plugins, wie beispielsweise Zenarmor für NGFW-Features, sowie eine fachgerechte Konfiguration der entsprechenden Dienste.

Administrative Effizienz: In Bezug auf die Verwaltung zeigt sich eine deutliche Differenzierung der Konzepte. Während Sophos durch das Prinzip des „Management by Exception“ und eine zentrale Cloud-Verwaltung die tägliche Administrationszeit verkürzt und durch Automatisierung Fehlerquellen minimiert, verlangt OPNsense tiefgehende Fachkenntnisse. Die Administration der Open-Source-Lösung ist manueller geprägt und erfordert vom Personal ein detailliertes Verständnis der zugrunde liegenden Protokolle und Regelsätze.

Wirtschaftlichkeit: Die Analyse der TCO über einen Zeitraum von drei Jahren belegt, dass sich die Gesamtkosten beider Lösungen nahezu ausgleichen. Es wurde jedoch deutlich, dass sich die Kostenstruktur signifikant verschiebt: Weg von hohen, wiederkehrenden Lizenzgebühren an den Hersteller hin zu einem erhöhten personellen Aufwand für Wartung, Monitoring und die notwendige Absicherung durch SLAs. Das IT-Dienstleistungsunternehmen investiert somit weniger in Software-Nutzungsrechte, sondern primär in Know-how und die individuelle Betreuung der Infrastruktur.

6.2 Beantwortung der Forschungsfragen

Um die zentrale Zielsetzung dieser Arbeit zu bewerten, werden im Folgenden, die eingangs formulierten Forschungsfragen auf Basis der technischen Evaluation und der Wirtschaftlichkeitsanalyse beantwortet.

Ist es möglich, proprietäre Firewall-Systeme durch Open-Source-Lösungen wie OPNsense zu ersetzen, ohne Abstriche bei der Sicherheit zu machen?

- Ja, eine Substitution ist technisch ohne Sicherheitsverlust möglich.
- Die Evaluation hat gezeigt, dass OPNsense durch die Integration von Plugins wie Zenarmor und Engines wie Suricata alle geforderten NGFW-Features (DPI, IDS/IPS, TLS-Inspection, Webfilter, etc.) auf dem Stand der Technik abbilden kann.
- Die Sicherheit wird hierbei nicht durch das Produkt gemindert, sondern hängt maßgeblich von der fachgerechten Konfiguration und der kontinuierlichen Pflege der Regelsätze ab.

Wie verhält sich das Kosten-Nutzen-Verhältnis bei der Nutzung von OPNsense im Vergleich zu Sophos XGS?

- OPNsense bietet ein überlegenes Preis-Leistungs-Verhältnis hinsichtlich der Lizenzkosten, erfordert jedoch eine Reinvestition der Ersparnis in personelle Ressourcen.
- Während die Investitionskosten (CAPEX) beider Lösungen auf einem ähnlichen Niveau liegen, gleichen sich auch die Betriebskosten (OPEX) über den Betrachtungszeitraum an. Infolgedessen bleiben die Gesamtkosten (TCO) über drei Jahre nahezu identisch, da die geringeren Lizenzgebühren der OPNsense durch den höheren manuellen Wartungsaufwand neutralisiert werden.
- Der Nutzen liegt primär in der Unabhängigkeit von Lizenzmodellen und der Wertschöpfung durch den Aufbau von lokalem Expertenwissen.

Unter welchen Bedingungen ist die Entscheidung für eine Open-Source-Lösung für ein KMU rentabel und sinnvoll?

- Eine Open-Source-Lösung ist dann sinnvoll, wenn das IT-Dienstleistungsunternehmen entweder schon über internes Know-how verfügt oder sich von Lizenzgebühren und Vendor Lock lösen möchte.
- Rentabel ist die Lösung insbesondere für Unternehmen, die Flexibilität bei der Hardwarewahl (z. B. Nutzung von Standard-PCs) schätzen und eine transparente Sicherheitsarchitektur (Open Source) gegenüber Black-Box-Systemen bevorzugen.
- Für Kleinstunternehmen ohne jegliche IT-Betreuung bleibt eine proprietäre Lösung wie Sophos aufgrund der umfassende Komplettlösung oft die pragmatischere, wenn auch teurere Wahl.

Kann OPNsense die rechtlichen Anforderungen (DSGVO, NIS2) ebenso erfüllen wie kommerzielle Anbieter?

- Ja, sofern der Betrieb durch professionelle Service-Prozesse (Patch-Management, Monitoring) gedeckt wird.
- Die technische Compliance (Integrität und Vertraulichkeit) ist durch die dokumentierten Security-Features gegeben.
- Die notwendige Haftung und Garantie werden bei OPNsense erfolgreich vom Hersteller auf den qualifizierten Dienstleistenden verlagert, was die rechtliche Sorgfaltspflicht gegenüber den Aufsichtsbehörden erfüllt.

6.3 Ausblick auf zukünftige Arbeiten

Die vorliegende Arbeit konzentriert sich auf die grundlegende Evaluation von OPNsense als Alternative zu proprietären Systemen im KMU-Umfeld. Aufbauend auf diesen Ergebnissen ergeben sich verschiedene Forschungs- und Entwicklungsfelder, die das Potenzial haben, die Effizienz und Skalierbarkeit der vorgestellten Lösung weiter zu steigern:

Automatisierung durch Infrastructure as Code (IaC): Eine tiefergehende Untersuchung könnte klären, wie OPNsense-Konfigurationen mittels Tools wie Ansible oder Terraform automatisiert ausgerollt und versioniert werden können. Dies würde den initialen Setup-Aufwand reduzieren und den in dieser Arbeit ermittelten administrativen Wartungsaufwand (TCO) signifikant senken.

Zentrale Verwaltung und Multi-Mandanten-Fähigkeit: Um als Dienstleistungsunternehmen eine größere Anzahl an KMU-Kunden effizient zu betreuen, ist die Evaluation von zentralen Management-Plattformen wie OPNcentral oder Cloud-basierten Monitoring-Lösungen (z. B. InfluxDB und Grafana) notwendig. Ziel wäre es, eine vergleichbare Übersichtlichkeit wie bei Sophos Central zu erreichen.

Virtualisierung und Cloud-Szenarien: Während in dieser Arbeit dedizierte Hardware im Fokus stand, bietet der Vergleich von virtualisierten Firewall-Instanzen unter Proxmox oder ESXi spannende Ansätze für moderne Rechenzentrumsstrukturen. Hierbei könnte die Flexibilität bei Backup- und Desaster-Recovery-Szenarien im Vergleich zu physischen Appliances untersucht werden.

KI-gestützte Incident-Analyse: Ein zukunftsweisender Ansatz liegt in der Integration von künstlicher Intelligenz zur Log-Analyse. Durch automatisierte Mustererkennung könnte die derzeit noch reaktive Suche in OPNsense-Protokollen transformiert werden, um den Usability-Nachteil gegenüber den proaktiven Alarmierungssystemen kommerzieller Anbieter auszugleichen.

Optimierung des Managed-Service-Modells: Schließlich wäre eine detaillierte Ausarbeitung verschiedener Dienstleistungspakete (SLA-Stufen) sinnvoll, um den finanziellen Vorteil der OPNsense-Lösung noch präziser in skalierbare Geschäftsmodelle für IT-Dienstleistungsunternehmen zu übersetzen.

Literaturverzeichnis

BSI (2023): BSI IT-Grundschutz-Kompendium. Bonn: Online im Internet: URL: https://www.bsi.bund.de

„Cybersecurity as a Service Delivered“ (o. J.): SOPHOS. Cybersecurity as a Service Delivered. Online im Internet: URL: https://www.sophos.com/en-us/company (Zugriff am: 11.05.2026).

„DEC740 – OPNsense® Desktop Security Appliance“ (o. J.): DEC740 – OPNsense® Desktop Security Appliance. Online im Internet: URL: https://shop.opnsense.com/product/dec740-opnsense-desktop-security-appliance/ (Zugriff am: 18.05.2026).

„Download“ (o. J.): OPNsense. Download. Online im Internet: URL: https://opnsense.org/download/ (Zugriff am: 10.03.2026).

„Download Anti Malware Testfile“ (o. J.): EICAR. Download Anti Malware Testfile. Online im Internet: URL: https://www.eicar.org/download-anti-malware-testfile/ (Zugriff am: 07.05.2026).

„Download pfSense Community Edition“ (o. J.): Download pfSense Community Edition. Online im Internet: URL: https://www.pfsense.org/download/ (Zugriff am: 10.03.2026).

„FreeBSD 14.1-RELEASE Errata“ (o. J.): The FreeBSD Project. FreeBSD 14.1-RELEASE Errata. Online im Internet: URL: https://www.freebsd.org/releases/14.1R/errata/ (Zugriff am: 19.05.2026).

GmbH, ito consult (o. J.-a): UTMshop. Sophos Firewall SW/Virtual: Xstream Protection Bundle Renewal. Online im Internet: URL: https://utm-shop.de/firewall/sophos/software-xgs-software-sg/sophos-software-xgs/renewals/sophos-firewall-sw-virtual-xstream-protection-bundle-renewal/xs1c4z12zzrcaa/laufzeit-1-jahr/anzahl-core-ram-1-core-unl-ram (Zugriff am: 27.04.2026).

GmbH, ito consult (o. J.-b): UTMshop. Sophos XGS 118 Security Appliance kaufen. Online im Internet: URL: https://utm-shop.de/firewall/sophos/sophos-xgs/xgs-118/ (Zugriff am: 27.04.2026).

Hickman, B. u.a. (2003): RFC 3511: Benchmarking Methodology for Firewall Performance. IETF. Online im Internet: URL: https://datatracker.ietf.org/doc/html/rfc3511

„Intrusion Prevention System — OPNsense documentation“ (o. J.): Intrusion Prevention System — OPNsense documentation. Online im Internet: URL: https://docs.opnsense.org/manual/ips.html#ids-and-ips (Zugriff am: 22.04.2026).

James, Hayden (2025): LinuxBlog.io. pfSense Firewall 2.8: Install & Config – Settings Walkthrough. Online im Internet: URL: https://linuxblog.io/pfsense-firewall-config-settings/ (Zugriff am: 18.05.2026).

„Keine RAM-Beschränkung mehr bei Sophos Virtual, Software und Cloud Firewalls – Sophos Partner News“ (o. J.): Keine RAM-Beschränkung mehr bei Sophos Virtual, Software und Cloud Firewalls – Sophos Partner News. Online im Internet: URL: https://partnernews.sophos.com/de-de/2025/03/products/sophos-firewall-virtual-software-cloud-ram-licensing-update/ (Zugriff am: 18.05.2026).

Ltd, Sophos (o. J.-a): Ablauf der Firewall-Lizenz - Sophos Central Admin. Online im Internet: URL: https://docs.sophos.com/central/customer/help/de-de/LicensingGuide/FirewallLicenses/LicenseExpiration/ (Zugriff am: 05.05.2026).

Ltd, Sophos (o. J.-b): Enhanced - Sophos Support. Online im Internet: URL: https://docs.sophos.com/support/help/de-de/services-guide/enhanced/ (Zugriff am: 11.05.2026).

Ltd, Sophos (o. J.-c): Severity levels of IPS signatures - Sophos Firewall. Online im Internet: URL: https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/IntrusionPrevention/IPSPolicies/IPSSignatureSeverityDefinitions/ (Zugriff am: 18.05.2026).

„Netgate Forum“ (o. J.): Netgate Forum. Netgate Forum. Online im Internet: URL: https://forum.netgate.com (Zugriff am: 18.05.2026).

„Netgate Global Support“ (o. J.): Netgate Global Support. Online im Internet: URL: https://www.netgate.com/support (Zugriff am: 04.03.2026).

„Netgate Store“ (o. J.): Netgate. Netgate Store. Online im Internet: URL: https://shop.netgate.com/ (Zugriff am: 10.03.2026).

„OPNsense® Business Edition 1yr subscription“ (o. J.): OPNsense® Business Edition 1yr subscription. Online im Internet: URL: https://shop.opnsense.com/product/opnsense-business-edition/ (Zugriff am: 27.04.2026).

„OPNsense“ (o. J.): GitHub. OPNsense. Online im Internet: URL: https://github.com/opnsense (Zugriff am: 11.05.2026).

„OPNsense 24.7.1 released“ (o. J.): OPNsense Forum. OPNsense 24.7.1 released. Online im Internet: URL: https://forum.opnsense.org/index.php?topic=42046.0 (Zugriff am: 19.05.2026).

„OPNsense Forum - Index“ (o. J.): OPNsense Forum. OPNsense Forum - Index. Online im Internet: URL: https://forum.opnsense.org/index.php (Zugriff am: 18.05.2026).

„OPNsense Reddit Community“ (o. J.): OPNsense Reddit Community. Online im Internet: URL: https://www.reddit.com/r/opnsense/

„OPNsense-Whitepaper-features-NIEUW.pdf“ (o. J.): OPNsense-Whitepaper-features-NIEUW.pdf. Online im Internet: URL: https://opnsense.org/wp-content/uploads/2025/11/OPNsense-Whitepaper-features-NIEUW.pdf (Zugriff am: 14.04.2026).

„pfSense Plus Features“ (o. J.): pfSense Plus Features. Online im Internet: URL: https://www.netgate.com/pfsense-features (Zugriff am: 14.04.2026).

„pfSense Reddit Community“ (o. J.): pfSense Reddit Community. Online im Internet: URL: https://www.reddit.com/r/PFSENSE/

„Product categories Hardware“ (o. J.): Product categories Hardware. Online im Internet: URL: https://shop.opnsense.com/product-categorie/hardware-appliances/ (Zugriff am: 04.03.2026).

„Product categories Support“ (o. J.-a): Product categories Support. Online im Internet: URL: https://shop.opnsense.com/product-categorie/support/ (Zugriff am: 04.03.2026).

„Product categories Support“ (o. J.-b): Product categories Support. Online im Internet: URL: https://shop.opnsense.com/product-categorie/support/ (Zugriff am: 05.05.2026).

„Releases | pfSense Documentation“ (o. J.): Releases | pfSense Documentation. Online im Internet: URL: https://docs.netgate.com/pfsense/en/latest/releases/index.html (Zugriff am: 14.04.2026).

„Releases — OPNsense documentation“ (o. J.): Releases — OPNsense documentation. Online im Internet: URL: https://docs.opnsense.org/releases.html (Zugriff am: 04.03.2026).

„Richtlinie (EU) 2022/2555“ (2022): Richtlinie (EU) 2022/2555. OJ L Online im Internet: URL: http://data.europa.eu/eli/dir/2022/2555/oj (Zugriff am: 21.01.2026).

Scarfone, Karen; Mell, Peter (2007): NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology. Online im Internet: DOI: 10.6028/NIST.SP.800-94

„Sophos Endpoint IPS: Frequently asked questions“ (o. J.): Sophos Endpoint IPS: Frequently asked questions. Online im Internet: URL: https://support.sophos.com/support/s/article/KBA-000006910?language=en_US (Zugriff am: 22.04.2026).

„Sophos UTM: Low throughput with Intrusion Prevention (IPS)“ (o. J.): Sophos UTM: Low throughput with Intrusion Prevention (IPS). Online im Internet: URL: https://support.sophos.com/support/s/article/KBA-000002957?language=en_US (Zugriff am: 18.05.2026).

Souppaya, Murugiah; Scarfone, Karen (2012): Guidelines on Firewalls and Firewall Policy. National Institute of Standards and Technology (NIST). Online im Internet: DOI: 10.6028/NIST.SP.800-41r1

Tanenbaum, Andrew S.; Feamster, Nick; Wetherall, David J. (2021): Computer Networks. 6th Aufl. Harlow, England: Pearson.

„Verordnung (EU) 2016/679“ (2016): Verordnung (EU) 2016/679. OJ L Online im Internet: URL: http://data.europa.eu/eli/reg/2016/679/oj (Zugriff am: 21.01.2026).

(2002): „The cathedral and the bazaar: musings on Linux and open source by an accidental revolutionary“ (2002): In: Choice Reviews Online, 39 (2002), 05, S. 39-2841-39–2841. Online im Internet: DOI: 10.5860/CHOICE.39-2841