INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
REDE DE COMPUTADORES
CAMPUS MACAPÁ

CAIO ROBERTO DE SOUZA TEIXEIRA

CONTRIBUIÇÃO DO FIREWALL *Pfsense* PARA SEGURANÇA DA INFORMAÇÃO E CONTROLE DE ACESSO EM REDES CORPORATIVAS DE PEQUENO PORTE

MACAPÁ
2026

CAIO ROBERTO DE SOUZA TEIXEIRA

CONTRIBUIÇÃO DO FIREWALL PfSense PARA SEGURANÇA DA INFORMAÇÃO E CONTROLE DE ACESSO EM REDES CORPORATIVAS DE PEQUENO PORTE

Trabalho de Conclusão de Curso apresentado à coordenação do curso Tecnologia em Rede de Computadores como requisito avaliativo para obtenção do título de Tecnólogo em Rede de Computadores.
Orientador: Esp. José Anderson Carvalho Brasil.

MACAPÁ
2026

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

T266c Teixeira, Caio Roberto de Souza
Contribuição do firewall pfsense para segurança da informação e controle de acesso em redes corporativas de pequeno porte / Caio Roberto de Souza Teixeira - Macapá, 2026.
42 f.: il.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Tecnologia em Redes de Computadores, 2026.

Orientador: José Anderson Carvalho Brasil.

1. Segurança da informação. 2. Firewall. 3. Pfsense. I. Brasil, José Anderson Carvalho, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

CAIO ROBERTO DE SOUZA TEIXEIRA

CONTRIBUIÇÃO DO FIREWALL PfSense PARA SEGURANÇA DA INFORMAÇÃO E CONTROLE DE ACESSO EM REDES CORPORATIVAS DE PEQUENO PORTE

Trabalho de Conclusão de Curso apresentado à coordenação do curso Tecnologia em Rede de Computadores como requisito avaliativo para obtenção do título de Tecnólogo em Rede de Computadores.

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br
JOSE ANDERSON CARVALHO BRASIL
Data: 20/07/2026 15:20:29-0300
Verifique em https://validar.iti.gov.br

Prof. Esp. José Anderson Carvalho Brasil (Orientador)

Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Documento assinado digitalmente
gov.br
LOURIVAL QUEIROZ ALCANTARA JUNIOR
Data: 04/08/2026 10:49:49-0300
Verifique em https://validar.iti.gov.br

Prof. Me. Lourival Queiroz Alcântara Júnior

Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Documento assinado digitalmente
gov.br
SHIRLEY DA COSTA MONTEIRO
Data: 18/07/2026 20:32:46-0300
Verifique em https://validar.iti.gov.br

Prof.ª Esp. Shirley da Costa Monteiro

Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Apresentado em: 11 / 06 / 2025.

Conceito/Nota: 95

Aos meus pais que não mediram esforços para que eu tivesse uma educação baseada em adquirir conhecimentos.

AGRADECIMENTOS

Ao meu orientador José Anderson Brasil

A minha família, pelo incentivo de nunca desistir de alcançar meus objetivos.

Aos professores que sempre apoiaram minha formação no curso de redes.

“O principal processo da escola é o ensino aprendizagem e o principal agente deste processo é o professor.”

(COUTINHO, 2021, p.109).

RESUMO

A segurança da informação tem se consolidado como um elemento fundamental para a proteção dos ativos digitais e para a continuidade das operações organizacionais em um cenário marcado pelo aumento das ameaças cibernéticas e pela crescente dependência das tecnologias da informação. Nesse contexto, os firewalls desempenham papel estratégico na proteção de redes corporativas, permitindo o controle de acessos, a filtragem do tráfego de dados e a implementação de políticas de segurança. Entre as diversas soluções disponíveis, o PfSense destaca-se como uma plataforma de código aberto amplamente utilizada para gerenciamento e proteção de redes, oferecendo recursos avançados de firewall, roteamento, redes privadas virtuais (VPN), monitoramento e segmentação de tráfego. Diante disso, o presente trabalho teve como objetivo analisar como a utilização do firewall PfSense pode contribuir para o aumento da segurança e do controle de acessos em redes corporativas de pequeno porte por meio do uso de hardware de baixo custo. Quanto à metodologia, a pesquisa caracteriza-se como básica, de abordagem qualitativa, com objetivos descritivos e exploratórios, desenvolvida por meio de pesquisa bibliográfica. A coleta de dados foi realizada a partir da análise de livros, artigos científicos, trabalhos acadêmicos e documentos técnicos relacionados à segurança da informação, firewalls, software livre e à plataforma PfSense. Os resultados evidenciaram que os firewalls constituem mecanismos essenciais para a proteção de ambientes computacionais, atuando na prevenção de acessos não autorizados e na mitigação de ameaças digitais. Verificou-se ainda que o modelo Open Source oferece vantagens relacionadas à transparência, flexibilidade e redução de custos, favorecendo sua adoção por organizações com recursos limitados. Em relação ao PfSense, constatou-se que a ferramenta reúne funcionalidades robustas de segurança e pode ser implementada em equipamentos de baixo custo, apresentando-se como uma alternativa tecnicamente eficiente e economicamente viável para pequenas empresas. Conclui-se que o PfSense representa uma solução relevante para o fortalecimento da segurança de redes corporativas, contribuindo para o controle de acessos, a proteção das informações e a melhoria da gestão da segurança da informação em ambientes organizacionais.

Palavras-chave: segurança da informação; firewall; PfSense.

ABSTRACT

Information security has become a fundamental element for protecting digital assets and ensuring the continuity of organizational operations in a scenario marked by increasing cyber threats and growing dependence on information technologies. In this context, firewalls play a strategic role in protecting corporate networks, enabling access control, data traffic filtering, and the implementation of security policies. Among the various solutions available, PfSense stands out as a widely used open-source platform for network management and protection, offering advanced firewall, routing, virtual private network (VPN), monitoring, and traffic segmentation features. Therefore, this study aimed to analyze how the use of the PfSense firewall can contribute to increased security and access control in small corporate networks through the use of low-cost hardware. Regarding methodology, the research is characterized as basic, with a qualitative approach, descriptive and exploratory objectives, developed through bibliographic research. Data collection was carried out through the analysis of books, scientific articles, academic papers, and technical documents related to information security, firewalls, open-source software, and the PfSense platform. The results showed that firewalls are essential mechanisms for protecting computing environments, acting to prevent unauthorized access and mitigate digital threats. It was also found that the Open Source model offers advantages related to transparency, flexibility, and cost reduction, favoring its adoption by organizations with limited resources. Regarding PfSense, it was found that the tool combines robust security functionalities and can be implemented on low-cost equipment, presenting itself as a technically efficient and economically viable alternative for small businesses. It is concluded that PfSense represents a relevant solution for strengthening the security of corporate networks, contributing to access control, information protection, and improved information security management in organizational environments.

Keywords: information security; firewall; PfSense.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A dependência de recursos tecnológicos em ambientes organizacionais torna a segurança da informação um fator essencial para a continuidade dos serviços e proteção de dados corporativos. Pequenas e médias empresas frequentemente enfrentam dificuldades para implementar soluções robustas de segurança devido aos altos custos de equipamentos e softwares proprietários, além da limitação de equipes esp ecializadas. Há ainda a inexistência de políticas adequadas de segurança, segmentação de rede e controle de acessos, elucidando um ambiente corporativo com vulnerabilidades que podem comprometer a integridade, confidencialidade e disponibilidade das informações.

Com o avanço das tecnologias digitais, as redes corporativas se tornaram elementos essenciais para o funcionamento das organizações, independentemente do seu porte, a utilização de recursos tecnológicos destinados ao armazenamento de informações, comunicação interna e externa e acesso aos serviços em nuvem, estão cada vez mais presentes nos ambientes corporativos (Barbosa; Reis, 2012; Milani; Dian, 2025). Por outro lado, essa utilização também aumentou riscos de acessos não autorizados, invasão e ataques de malware e vazamento de dados, evidenciando a necessidade de implementação de mecanismo de segurança de rede, visando garantir a confidencialidade, integridade e disponibilidade das informações (Ferreira, 2024; Fontanetti, 2018).

Entre os mecanismos de segurança de rede existentes, os firewalls se apresentam como uma estratégia para o controle do tráfego de dados entre redes internas e externas, permitindo a definição de políticas de acesso e proteção contra ameaças cibernéticas (Ferreira, 2024; Lopez, 2020). Entretando, no âmbito das pequenas empresas existem limitações orçamentárias que dificultam a adoção de equipamentos e softwares proprietários de segurança que, geralmente, possuem alto custo de licenciamento e manutenção (Godoy, 2016). Esse cenário evidencia a necessidade de alternativas que ofertam um nível adequado de proteção sem comprometer a sustentabilidade financeira das organizações (Rossi; Bochnia, 2024).

A pesquisa foi desenvolvida a partir de um estudo de caso realizado em uma empresa de pequeno porte localizada no município de Macapá-AP, cuja infraestrutura de Tecnologia da Informação apresentava limitações relacionadas à segurança da informação e ao gerenciamento da rede corporativa. Durante o diagnóstico inicial, constatou-se que a organização dependia integralmente do roteador fornecido pela empresa responsável pelo serviço de internet, que realizava remotamente configurações críticas da rede. Também foram identificadas vulnerabilidades decorrentes da inexistência de segmentação entre a rede

corporativa e a rede destinada aos visitantes, ausência de mecanismos centralizados de autenticação de usuários, compartilhamento de arquivos sem controle adequado de permissões e armazenamento de documentos importantes em computadores locais, elevando os riscos de acessos não autorizados e perda de dados.

Diante desse cenário, a empresa foi escolhida como objeto do estudo por representar a realidade de muitas pequenas organizações que possuem infraestrutura tecnológica limitada e enfrentam dificuldades para investir em soluções proprietárias de segurança. A implantação do firewall PfSense foi acompanhada por uma reestruturação parcial da infraestrutura de rede, contemplando a segmentação dos ambientes, implementação de VPN para acesso remoto seguro, virtualização de servidores, implantação de serviços de diretório, gerenciamento centralizado de usuários e adoção de políticas de controle de acesso. Essas ações possibilitaram avaliar, em um ambiente real, a contribuição do PfSense para o fortalecimento da segurança da informação, melhoria do gerenciamento da rede e redução das vulnerabilidades existentes, reforçando a pertinência da aplicação prática apresentada neste estudo.

Nesse contexto, ferramentas open source surgem como alternativas viáveis de código aberto para gerenciamento e proteção de redes corporativas, dentre elas, destaca-se o PfSense, um firewall baseado em FreeBSD amplamente utilizado para gerenciamento e controle de tráfego de rede (Dourado, 2022). Essa plataforma oferece recursos avançados de firewall, controle de acesso, monitoramento de tráfego, redes privadas virtuais (VPN), proxy, filtragem de conteúdo e segmentação de rede, que podem ser executados com baixo custo (Neves; Machado; Centenaro, 2014). Dessa forma se apresenta como uma alternativa acessível para as pequenas empresas que buscam fortalecer sua infraestrutura de segurança sem realizar grandes investimentos (Lopez, 2020).

Diante desse cenário, este estudo buscou responder como a implantação do PfSense em uma rede corporativa de pequeno porte pode contribuir para o aumento da segurança e controle do acesso, utilizando equipamentos de baixo custo. A compreensão dos benefícios, limitações e resultados dessa implementação pode fornecer subsídios para a adoção de soluções economicamente viáveis e tecnicamente eficazes no contexto da segurança de redes corporativas.

Dessa forma, este estudo tem como objetivo geral analisar como a utilização do firewall PfSense pode contribuir para o aumento da segurança e controle do acesso em redes corporativas de pequeno porte por meio do uso de hardware de baixo custo. Buscou-se especificamente, descrever os conceitos fundamentais de segurança da informação, firewalls e

controle de segurança em redes corporativas, destacando a sua importância para a proteção dos ativos informacionais; apresentar as características, funcionalidades e recursos do firewall PfSense como solução open source para a segurança e gerenciamento de redes; e discutir sobre as contribuições, vantagens e limitações da utilização do PfSense em pequenas empresas que buscam soluções de segurança de baixo custo.

A relevância deste estudo está na análise prática da implantação do PfSense em uma rede corporativa de pequeno porte, tendo em vista a avaliação da sua eficácia na proteção de ativos de informação e gerenciamento de acessos à rede pode contribuir para a disseminação de soluções tecnológicas acessíveis e eficientes, auxiliando gestores e profissionais de tecnologias em suas tomadas de decisões relativas à segurança da informação. Portanto, este estudo justifica-se pela necessidade de ampliação do conhecimento sobre a aplicação de ferramentas de código aberto em ambientes corporativos, principalmente no contexto de pequenas empresas que apresentam recursos limitados para o investimento tecnológico. Sendo assim, este trabalho busca demonstrar a possibilidade de elevação do nível de segurança de uma rede corporativa por meio de soluções economicamente viáveis, sem comprometer a eficiência e a confiabilidade dos serviços ofertados.

2 SEGURANÇA DA INFORMAÇÃO E UTILIZAÇÃO DE TECNOLOGIAS PARA PROTEÇÃO DE REDES CORPORATIVAS

A segurança da informação pode ser entendida como um conjunto de práticas, políticas, tecnologias e procedimentos que buscam proteger os ativos informacionais de uma organização contra ameaças internas e externas (Alves; Souza, 2022). Como o avanço das tecnologias digitais e aumento da dependência dos sistemas computacionais, a proteção das informações se apresenta como um elemento fundamental para empresas de todos os portes (Ferreira, 2024). A segurança da informação garante a proteção contra acessos não autorizados, alterações indevidas, perdas acidentais e interrupções de disponibilidade. Sua aplicação envolve aspectos tecnológicos, bem como fatores humanos e organizacionais (Fontanetti, 2018).

A norma ABNT NBR ISO/IEC 2700 define a segurança da informação como preservação da confidencialidade, integridade e disponibilidade das informações, esses princípios são denominados de tríade CIA (Confidentiality, Integrity and Availability), constituindo-se como a base para estratégias de proteção de dados (ABNT, 2022). Em linhas gerais, a confidencialidade assegura o acesso às informações apenas para pessoas autorizadas, a integridade garante que os dados permaneçam corretos sem alterações indevidas, a disponibilidade assegura o acesso aos recursos sempre que necessário (Biondo; Morcelli; Neitzek, 2023).

A confidencialidade é um dos pilares essenciais que garante a segurança da informação, principalmente em ambientes corporativos que operam com informações sensíveis. Organizações que utilizam mecanismos como autenticação, criptografia, controle de acesso e segmentação de redes, garantem a segurança e o controle de acesso às informações, reduzindo riscos de vazamento de dados e impedimento de acesso a usuários não autorizados (Cicoli; Batistão, 2025). A proteção da confidencialidade é uma estratégia relevante frente às ameaças cibernéticas e necessidade de conformidade com legislações de proteção de dados (Ferreira, 2024).

A integridade das informações garante que os dados não sejam modificados indevidamente, tendo em vista que durante o seu armazenamento, processamento ou transmissão podem ocorrer falhas que geram consequências graves para uma organização, como prejuízo financeiros e comprometimento da tomada de decisões (Cicoli; Batistão, 2025). Mecanismos como assinaturas digitais, funções de hash, sistemas de auditoria e controle de alteração, buscam evitar esses problemas, assegurando que as informações mantenham sua precisão e confiabilidade ao longo do tempo (Ferreira, 2024).

A disponibilidade diz respeito à capacidade de acessar informações e serviços sempre que necessário, visto que em ambientes corporativos a indisponibilidade de sistemas interrompe processos essenciais, causando impactos significativos nas operações (Fontanelli, 2018). Fatores como ataques cibernéticos, falhas de hardware, desastres naturais, erros humanos, podem afetar a disponibilidade de informações (Ferreira, 2024). Nesse contexto, adotar estratégias de redundância, backups, monitoramento contínuo e planos de recuperação de desastres, diminuem riscos e garantem a continuidade dos serviços (Nascimento, 2023).

Além da CIA, há outros elementos complementares que podem ser incorporados ao princípio de segurança da informação como autenticidade, responsabilidade e não repúdio. A autenticidade busca garantir legitimidade à identidade de usuários, sistemas e informações (Barbosa; Reis, 2012). A responsabilidade diz respeito à capacidade de identificar e registrar ações realizadas pelos usuários e o não repúdio impede que uma parte negue a autoria de uma ação previamente executada. Esses princípios ampliam a capacidade das organizações de controlar e auditar seus ambientes tecnológicos (Cicoli; Batistão, 2025).

A origem das ameaças à segurança da informação inclui diversos fatores, internos e externos, que representam riscos significativos para a proteção dos ativos informacionais das organizações. Dentre os fatores internos, destaca-se erros operacionais, negligência, uso inadequado de recursos tecnológicos ou ações maliciosas praticadas por colaboradores. Entre as ameaças externas estão os ataques e invasões de software maliciosos (malware) que sequestram dados ou dispositivos impedindo o acesso a arquivos (ransomware), geralmente por meio de links fraudulentos em e-mails ou downloads acidentais (phishing) (Ferreira, 2024).

Dentro da segurança da informação, a gestão de riscos é uma atividade essencial que permite identificar vulnerabilidades, avaliar ameaças e implementar controles que reduzem a probabilidade de incidentes (Ferreira, 2024). Esse processo permite que as organizações direcionem seus recursos de forma eficiente, avaliando riscos mais relevantes para suas operações por meio de metodologias que contribuem para a criação de um ambiente seguro e preparado para enfrentar desafios relacionados à segurança digital (Nascimento, 2023). Outro aspecto relevante é conscientização dos usuários, uma vez que boa parte dos incidentes ocorre devido às falhas humanas como uso abertura de arquivos maliciosos ou compartilhamento inadequado de informações (Dourado, 2022). Nesse contexto, programas de treinamento e campanhas de conscientização se apresentam como componentes essenciais das estratégias de proteção, reduzindo significativamente vulnerabilidades organizacionais (Ferreira, 2024).

Contudo, a segurança da informação é um requisito indispensável em ambientes tecnológicos, garantindo a sustentabilidade das organizações, nesse contexto, a implementação de políticas, controles e tecnologias adequadas promove a redução de riscos, proteção de rede e garantia da continuidade dos negócios (Evangelista, 2014). Portanto, ferramentas de proteção de rede como firewalls e sistemas de controle de acesso desempenham um papel fundamental na construção de ambientes corporativos seguros, constituindo-se como elementos essenciais para a proteção de informações e recursos computacionais (Cicoli; Batistão, 2025).

2.1 Utilização do Firewall como mecanismo de proteção e controle de acesso em redes corporativas

O firewall é uma das principais ferramentas utilizadas para a proteção de redes computacionais, responsável por controlar o fluxo de dados entre diferentes ambientes de rede, seu funcionamento é baseado na análise e filtragem do tráfego que entra e sai de uma infraestrutura (Dourado, 2022). Atua como uma barreira de segurança entre redes confiáveis e não confiáveis, permitindo ou bloqueando conexões de acordo com regras estabelecidas previamente, sendo uma ferramenta indispensável de combate às ameaças cibernéticas em ambientes corporativos (Fachinelli; Ahlert, 2019). Auxilia também na implementação de políticas de segurança da informação, contribuindo para a redução de vulnerabilidades e proteção de ativos digitais, sendo considerado um componente essencial da infraestrutura de segurança (Ferreira, 2024).

Essa ferramenta surgiu na década de 1980 em resposta ao aumento expressivo de ameaças em redes conectadas à internet, inicialmente, realizavam apenas a filtragem simples de pacotes, analisando endereços de IP e portas de comunicação. Posteriormente, evolui para um mecanismo de proteção, incorporando inspeção de estado, análise de aplicações e detecção de comportamentos suspeitos. E, atualmente, oferecem recursos avançados de monitoramento e controle, permitindo maior prevenção de ataques (Milani; Dian, 2025).

A função principal de um firewall consiste em controlar o acesso entre diferentes redes por meio da aplicação de regras de filtragem que determinam os tipos de tráfego que serão permitidos ou bloqueados com base em parâmetros específicos como endereços de IP, protocolos de comunicação, portas de origem e destino e tipos de serviços utilizados. Esse processo restringe acessos indevidos, reduzindo a exposição da rede às ameaças externas, contribuindo para organização do tráfego corporativo, atuando como um mecanismo de prevenção contra riscos distintos (Fachinelli; Ahlert, 2019).

Podem ser classificados em diferentes categorias, conforme sua forma de funcionamento, entre os principais, destacam-se os firewalls de filtragem de pacotes, os de inspeção de estado e os de aplicação. Cada categoria apresenta características específicas em diferentes cenários de utilização, dependendo da necessidade de segurança das organizações (Lopez, 2020). Os modelos de filtragem analisam informação básicas de pacotes transmitidos, os de inspeção acompanham o contexto das conexões ativas e os de aplicação realizam análise mais detalhadas do conteúdo trafegado (Ferreira, 2024).

Os firewalls de inspeção monitoram o estado das conexões estabelecidas e verificam se os pacotes recebidos fazem parte de uma comunicação legítima, dessa forma, é possível identificar comportamentos anormais e bloquear conexões suspeitas com mais precisão (Neves; Machado; Centenaro, 2014). Além disso, reduzem a ocorrência de falsos positivos e aumentam a eficiência do controle de tráfego e permite gerenciar sessões de rede de modo inteligente. Essa funcionalidade está presente na maioria de firewalls corporativos, sua adoção fortalece a proteção de ambientes computacionais (Barbosa; Reis, 2012).

Outra categoria relevante é a de próxima geração, também conhecida como Next Generation Firewall (NGFW), essas soluções combinam funcionalidades tradicionais de filtragem com recursos avançados de inspeção profunda de pacotes, controle de aplicações e prevenção de intrusões. Essa categoria consegue identificar aplicações específicas independentemente das portas utilizadas, proporciona maior visibilidade do tráfego de rede e permite a integração com sistemas de inteligência contra ameaças. Além disso, amplia a proteção contra aos ataques, por isso é frequentemente utilizada em organizações de médio e grande porte (Fachinelli; Ahlert, 2019).

Os firewalls desempenham um papel importante na segmentação de redes corporativas, tendo em vista que permite dividir a infraestrutura em diferentes áreas lógicas, separando setores, usuários e serviços. Essa estratégia reduz a propagação de ameaças e limita o impacto de possíveis incidentes de segurança, sendo possível controlar a comunicação entre segmentos distintos (Cicoli; Batistão, 2025). Sendo assim, aumenta o nível de proteção de recursos críticos da organização, contribuindo para a melhoria do desempenho da rede, apresentando-se como uma estratégia que permite boas práticas de segurança (Ferreira, 2024).

São também utilizados como ferramentas para implementação de políticas de acesso à internet, onde as organizações podem restringir o uso de determinados sites, serviços ou aplicações que representam riscos à segurança ou produtividade (Evangelista, 2014). Esse controle permite prevenir infecções por malware, monitorar o comportamento de usuários na rede corporativa e cumprir normas internas da empresa (Ferreira, 2024). Os registros que são

gerados pelos firewalls podem ser utilizados em auditoria e investigações sobre acidente, entretanto, não podem ser considerados como uma solução isolada (Dourado, 2022).

A segurança da informação exige abordagens que atuam de modo integrado, envolvendo diferentes tecnologias e procedimentos complementares como antivírus, sistemas de detecção de intrusão, políticas de acesso e programas de conscientização (Godoy, 2016). Nesse contexto, o firewall representa apenas uma das barreiras de defesa existentes em ambientes corporativos, sua eficácia e eficiência dependem de configurações adequadas e atualizações constantes, para que assim possam diminuir riscos de segurança de modo contínuo (Milani; Dian, 2025).

Diante do contexto de ameaças cibernéticas, os firewalls se apresentam como elementos essenciais para a proteção das redes corporativas, onde sua capacidade de controlar acessos e monitorar comunicações contribuem para a preservação da confidencialidade, integridade e disponibilidade das informações (Ferreira, 2024). Essas ferramentas surgiram para atender demandas de ambientes complexos e conectados, a sua utilização fortalece a postura de segurança das organizações, reduzindo a probabilidade de prejuízos operacionais (Evangelista, 2016). Portanto, sua implementação é indispensável para a gestão da segurança da informação, constituindo-se como um mecanismo de defesa das infraestruturas digitais modernas.

2.2 Software livre e Open source como alternativas para soluções de segurança em rede.

O conceito de software livre surgiu a partir de um movimento voltado à promoção da liberdade dos usuários em relação aos programas computacionais, formalizado por Richard Stallman na década de 1980 por meio da criação da Free Software Foundation (Rossi; Bochnia, 2023). Esse movimento se baseia na perspectiva de que os usuários devem possuir liberdade para executar, estudar, modificar e redistribuir os programas (Evangelista, 2016). O seu objetivo principal é garantir a autonomia tecnológica e compartilhamento do conhecimento, buscando estimular a colaboração entre desenvolvedores e usuários (Nascimento, 2023). Esse modelo é utilizado como referência em diversos projetos de tecnologia, com ampla relevância no cenário da informática (Neves; Machado; Centenaro, 2014).

Embora compartilhe diversos princípios com o software livre, o movimento Open Source surge posteriormente com objetivo de ampliar a aceitação comercial dos softwares de código, enfatizando aspectos relacionados à qualidade, inovação e eficiência do

desenvolvimento colaborativo (Rossi; Bochnia, 2023). A Open Source Iniciative estabeleceu critérios para caracterizar um software aberto, dentre eles destaca-se a disponibilidade do código-fonte para análise e modificação (Barbosa; Reis, 2016). Essa abordagem favorece a transparência e aprimoramento contínuo das aplicações, incentivando a participação de comunidades de desenvolvimento, resultando em projetos com elevado nível de maturidade tecnológica (Biondo; Morcelli; Neitzek, 2023).

Uma das vantagens dos softwares livres e código aberto é a redução de custos com licenciamento, tendo em vista que esses programas podem ser utilizados sem pagamento de taxas recorrentes (Rossi; Bochnia, 2023). Tal característica é relevante para instituições públicas, organizações sem fins lucrativos e pequenas empresas, uma vez que a economia obtida pode ser direcionada para outras áreas e funcionalidades reduzindo a dependência de fornecedores específicos e contribuindo para uma gestão eficiente dos recursos tecnológicos, ampliando o acesso à inovação (Nascimento, 2023).

A transparência proporcionada pelo acesso código-fonte é outro benefício, a possibilidade de analisar o funcionamento interno de um software possibilita a identificação de vulnerabilidades, correção de falhas e adaptação de funcionalidades às necessidades específicas dos usuários (Rossi; Bochnia, 2023). Esse nível de controle se torna importante para sistemas voltados à segurança da informação, favorecendo auditorias independentes e processos de verificação de conformidade, aumentando a transparência e confiança dos usuários na tecnologia utilizada, fortalecendo a segurança e confiabilidade dos sistemas (Evangelista, 2016).

Um dos pilares fundamentais do desenvolvimento Open Source é a colaboração, esse modelo possibilita a identificação rápida de problemas e a implementação de melhorias constantes, resultando em projetos de código aberto com elevado nível de estabilidade e desempenho (Barbosa; Reis, 2016). O compartilhamento de conhecimento acelera os processos de inovação tecnológica, onde a participação de especialistas contribui para o aprimoramento e enriquecimento de soluções, favorecendo a evolução contínua de projetos (Biondo; Morcelli; Neitzek, 2023).

No âmbito corporativo, o uso de software livre tornou-se significativo nos últimos anos, onde diferentes empresas adotaram soluções abertas para servidores, banco de dados, sistemas operacionais e ferramentas de segurança (Rossi; Bochnia, 2023). A redução de custos, flexibilidade de customização e a independência tecnológica são os principais fatores que impulsionaram essa adoção, visto que muitos softwares livres ofertam suporte profissional por meio de empresas especializadas, proporcionado segurança operacional e

viabilidade econômica (Evangelista, 2016). Esse modelo tornou-se uma alternativa competitiva às soluções proprietárias, uma vez que seu uso está presente em organizações de todos os portes (Barbosa; Reis, 2016).

A segurança dos softwares Open Source é um frequente objeto de discussão, onde a disponibilidade do código fonte se apresenta como facilitador da exploração de vulnerabilidades por atacantes (Rossi; Bochnia, 2023). Entretanto, a sua transparência permite uma revisão constante por parte da comunidade, favorecendo a identificação e correção de falhas de segurança de modo rápido (Barbosa; Reis, 2016). Diversos projetos apresentam elevados padrões de proteção, onde a segurança depende mais da qualidade da gestão do projeto do que do modelo de licenciamento (Biondo; Morcelli; Neitzek, 2023).

O Linux, Apache, PostgreSQL e o LibreOffice estão entre os modelos mais conhecidos de software livre, sendo amplamente utilizados em ambientes acadêmicos, governamentais e corporativos, demonstrando que o modelo Open Source possui capacidade para produzir tecnologias robustas e confiáveis (Biondo; Morcelli; Neitzek, 2023). Muitos projetos como esses servem de base para produtos comerciais utilizados em larga escala, uma vez que são amplamente adotados, evidenciando a sua relevância no mercado tecnológico (Barbosa; Reis, 2016). Seus benefícios estão além da vantajosidade econômica e financeira, representam um importante instrumento de democratização do acesso ao conhecimento (Rossi; Bochnia, 2023).

No âmbito da segurança da informação, o software livre desempenha um papel estratégico, visto que possui diversas ferramentas e funcionalidades utilizadas para o monitoramento, análise de vulnerabilidades e proteção de redes são desenvolvidas sob licença abertas (Rossi; Bochnia, 2023). Esse permite a implementação de mecanismos de segurança avançados sem a necessidade de alto investimento financeiro, garantindo atualizações frequentes e melhorias (Evangelista, 2016). Além disso, promove a independência tecnológica e ampliação de possibilidades de personalização dos sistemas, alcançando dimensões econômicas e sociais, essas características tornam esse modelo relevante para as organizações que buscam eficiência e sustentabilidade, consolidando-se como um elemento fundamental no ecossistema tecnológico atual (Nascimento, 2023).

2.3 PfSense como plataforma de segurança em redes corporativas

O PfSense é uma plataforma de segurança de rede baseada no sistema operacional FreeBSD, distribuída sob licença Open Source, desenvolvido inicialmente em 2004 como uma alternativa livre para implementação de firewalls e roteadores corporativos (Dourado,

2022). Sua característica principal é a oferta de recursos avançados de segurança sem a necessidade de aquisição de equipamentos prioritários de alto custo (Godoy, 2016). Essa ferramenta pode ser instalada em computadores convencionais e dispositivos dedicados, sua flexibilidade contribui para a sua adoção em organizações de diferentes portes, sua interface gráfica facilita o gerenciamento dos serviços (Lopez, 2016).

A sua arquitetura foi desenvolvida para fornecer alto desempenho e estabilidade em ambientes de rede, baseia-se no mecanismo de filtragem de pacotes Packet Filter, originalmente criado para o sistema OpenBSD, ofertando controle eficiente sobre o tráfego de dados (Dourado, 2022). Essa tecnologia permite a criação de regras para o gerenciamento das comunicações, possibilitando o monitoramento em tempo real das conexões ativas (Lopez, 2016). Foi projetado para operar de modo contínuo em ambientes corporativos, sua robustez é reconhecida por profissionais da área de segurança como uma solução amplamente confiável (Godoy, 2016).

Uma de suas funcionalidades centrais diz respeito à implementação de firewall com inspeção de estado, permitindo acompanhar o contexto das conexões estabelecidas e tomar decisões mais precisas sobre o tráfego de rede (Neves; Machado; Centenaro, 2014). A sua análise não está limitada aos aspectos individuais, considera todo o histórico da comunicação, aumentando a capacidade de identificação de comportamentos suspeitos (Lopez, 2016). Reduz a ocorrência de bloqueios indevidos, melhorando a segurança sem comprometer a usabilidade dos serviços, favorecendo a eficiência operacional da rede (Dourado, 2022).

O PfSense oferece ainda suporte avançado para redes privadas virtuais (VPNs), permitindo que usuários remotos acessem recursos operacionais de forma segura por meio de conexões criptografadas (Godoy, 2016). Suporta diferentes protocolos, incluindo OpenVPN, IPsec e WireGuard, essa versatilidade permite atender a diversos cenários de conectividade, contribuindo para proteção de informações transmitidas pela internet, auxiliando na manutenção da segurança em ambientes distribuídos (Neves; Machado; Centenaro, 2014).

A sua capacidade de segmentação de redes por meio de VLANs é outro recurso relevante do PfSense, essa funcionalidade permite separa diferentes grupos de usuários e serviços dentro da mesma infraestrutura física (Alves; Souza, 2022). A segmentação reduz a propagação de ameaças e facilita o gerenciamento de recursos computacionais e possibilita a aplicação de políticas específicas para cada segmento da rede (Neves; Machado; Centenaro, 2014). Essa abordagem fortalece a segurança organizacional, isolando ambientes críticos, apresentando recursos adequados para a sua implementação (Lopez, 2016).

O monitoramento de tráfego se constitui como outra característica importante da plataforma, disponibiliza relatórios, gráficos e registros detalhados sobre a utilização da rede que auxiliam na identificação de gargalos, comportamentos anormais e possíveis incidentes de segurança (Godoy, 2016). Permitem ainda uma gestão mais eficiente dos recursos disponíveis, contribuindo para melhoria contínua da infraestrutura tecnológica (Neves; Machado; Centenaro, 2014).

A sua expansão pode ocorrer por meio de instalação de pacotes adicionais que ampliam suas funcionalidades, entre os mais utilizados destacam-se o Snort, Suricata, Squid e pfBlockerNG (Dourado, 2022). Essas extensões permitem a implementação de sistemas de detecção de intrusão, proxy web, bloqueio de conteúdos maliciosos e filtragem avançada de tráfego, possibilitando adaptações de acordo com as necessidades das organizações (Neves; Machado; Centenaro, 2014). Evita ainda a instalação de componentes desnecessários, onde a flexibilização representa uma de suas principais vantagens, permitindo a personalização do ambiente conforme requisitos específicos (Lopez, 2016).

Um dos fatores que contribui para a sua popularidade é a facilidade de administração, a sua interface intuitiva permite configurar regras, monitorar conexões e gerenciar serviços sem a necessidade de conhecimentos avançados em sistemas operacionais (Godoy, 2016). Essa característica reduz a complexidade de implantação e manutenção da plataforma, favorecendo a sua adoção por pequenas empresas com equipes reduzidas de tecnologia, ampliando as possibilidades de utilização da ferramenta (Dourado, 2022).

No contexto da segurança da informação o PsSense se apresenta como uma alternativa economicamente viável para proteção de redes corporativas, sua capacidade de integrar múltiplas funcionalidade em uma única plataforma reduz custos relativos à aquisição de equipamentos especializados (Godoy, 2016). A sua natureza Open Source elimina despesas com licenciamento de software, tornando-se uma solução atrativa para empresas de pequeno e médio porte, favorecendo a sua adoção (Lopez, 2016).

Além disso, destaca-se como solução de gerenciamento e segurança de ambientes computacionais, onde os recursos de firewall, VPN, segmentação, monitoramento e controle de acesso permitem a implementação de políticas de segurança (Dourado, 2022). Sua flexibilidade e baixo custo tornam a tecnologia acessível às organizações com diferentes níveis de investimento, demonstrando que pode ofertar uma ferramenta estratégica para a proteção da infraestrutura de rede com elevado padrão de qualidade e confiabilidade (Neves; Machado; Centenaro, 2014).

3 METODOLOGIA

Para alcançar os objetivos propostos, optou-se por desenvolver uma pesquisa bibliográfica e aplicada voltada à compreensão das contribuições do firewall PfSense para o fortalecimento da segurança e do controle de acesso em redes corporativas de pequeno porte. A pesquisa buscou reunir literaturas capazes de subsidiar a discussão do problema investigado, bem como fundamentar os conceitos relacionados à segurança da informação, firewall, software livre e soluções open source aplicadas à proteção de redes corporativas. Além do levantamento teórico, foi realizado um estudo de caso em uma organização de pequeno porte, no qual ocorreu a implantação prática do firewall PfSense e reestruturação parcial da infraestrutura de rede.

A aplicação do estudo de caso foi realizada em uma empresa de pequeno porte localizada no município de Macapá-AP, selecionada por apresentar características compatíveis com o objetivo da pesquisa, especialmente em relação às limitações de infraestrutura tecnológica e à necessidade de adoção de mecanismos de segurança da informação de baixo custo. Inicialmente, foi realizada uma visita técnica para levantamento das condições do ambiente computacional, contemplando a análise da topologia da rede, dos equipamentos existentes, dos serviços disponibilizados, das políticas de gerenciamento de usuários e dos mecanismos de proteção empregados. Esse diagnóstico permitiu identificar vulnerabilidades relacionadas ao controle de acesso, à segmentação da rede, ao gerenciamento de permissões e à dependência do equipamento fornecido pela empresa responsável pelo acesso à internet, fornecendo subsídios para o planejamento da solução proposta.

Com base nas informações obtidas durante o diagnóstico, foi elaborado um plano de intervenção contemplando a implantação do firewall PfSense e a reestruturação parcial da infraestrutura de rede da organização. A execução do estudo de caso compreendeu a instalação e configuração do firewall, definição de regras de filtragem de tráfego, implementação de acesso remoto seguro por VPN, segmentação da rede corporativa e da rede destinada aos visitantes, virtualização do servidor existente, implantação de serviços de diretório, gerenciamento centralizado de usuários e configuração de serviços complementares de monitoramento e controle da navegação. Após a conclusão das etapas de implantação, foram realizados testes de funcionamento, validação dos serviços implementados e treinamento dos colaboradores responsáveis pela administração da infraestrutura, possibilitando a avaliação prática da solução proposta em um ambiente corporativo real e sua aderência às necessidades da organização.

Quanto à natureza da pesquisa, classifica-se como aplicada, visto que buscou aplicar o conhecimento científico para solucionar um problema identificado (Marconi; Lakatos, 2022), relacionado à segurança da informação em um ambiente corporativo. Pesquisas aplicadas possuem como finalidade gerar conhecimentos voltados à solução de problemas específicos (Silva, 2024). A aplicação prática permitiu avaliar sua efetividade diante das necessidades da empresa estudada, contribuindo para a proposição de medidas que fortalecem a segurança da infraestrutura de rede e reduzem vulnerabilidades decorrentes da ausência de políticas adequadas de proteção e controle.

Em relação aos objetivos, esta pesquisa caracteriza-se como descritiva e exploratória, uma vez que busca identificar, registrar, analisar e descrever características relacionados ao objeto pesquisado em seu contexto e ampliar o conhecimento sobre um assunto específico e ainda pouco explorado (Silva, 2024). Dessa forma, a pesquisa busca apresentar características relacionadas à utilização do firewall PfSense em redes corporativas, proporcionar maior familiaridade com o problema investigado e ampliar a compreensão sobre a aplicação de soluções open source em ambientes organizacionais. Desse modo, o estudo contribuirá para identificação de vantagens e limitações relacionadas à utilização do PfSense em diferentes perspectivas.

Quanto à sua abordagem, este estudo classifica-se como qualitativo, pois focaliza a interpretação e compreensão dos fenômenos estudados, priorizando a análise, conceitos e relações presentes nos dados coletados (Silva, 2024). Não houve preocupação com mensuração estatística das informações, visto que o foco da análise está voltado para as contribuições da ferramenta para a segurança e gerenciamento da infraestrutura de rede. Sendo assim, o método qualitativo favorece a interpretação crítica dos resultados alcançados, possibilitando uma análise aprofundada do contexto investigado (Marconi; Lakatos, 2022).

No que diz respeito aos procedimentos técnicos, esta pesquisa caracteriza-se como um estudo de caso por ser desenvolvida a partir da investigação de uma situação real em uma organização de pequeno porte, permitindo a análise detalhada da implementação e utilização do firewall PfSense em seu ambiente de rede (Silva, 2024). O estudo de caso consiste em um método que possibilita o exame detalhado de um ou poucos objetos, proporcionando amplo e profundo conhecimento sobre o fenômeno estudado (Marconi; Lakatos, 2022). Nesse sentido, permite compreender fundamentos da segurança da informação e características do PfSense de modo amplo, considerando as particularidades e necessidades da organização analisada.

A coleta de dados foi realizada em etapas complementares que forneceram subsídios para o desenvolvimento da pesquisa: 1) Levantamento bibliográfico; 2) Diagnóstico da

infraestrutura existente; 3) Implementação da solução proposta; 4) Avaliação dos resultados. As etapas desenvolvidas possibilitaram a articulação entre os conhecimentos teóricos e práticos, permitindo compreender a aplicação do PfSense em ambiente organizacional.

A primeira etapa consistiu no levantamento bibliográfico, onde foram levantados livros, artigos científicos, teses, dissertações, monografias, normas técnicas e documentos institucionais relacionados ao tema do trabalho. A seleção das fontes considerou critérios de relevância, atualidade e aderência ao problema de pesquisa, objetivando reunir informações capazes de sustentar teoricamente o estudo. Priorizou-se referências amplamente reconhecidas e citadas na área de tecnologia da informação e publicadas nos últimos 15 anos, garantindo consistência e atualidade ao referencial teórico, com exceção às leis, decretos e/ou normativas. Para o levantamento especializado da literatura, utilizou-se os seguintes descritores: 1) Segurança da informação; 2) Firewall; 3) Controle de acesso; 4) Software livre; 5) Open source; 6) Segurança de redes; e 7) PfSense. Esses descritores foram utilizados de forma isolada e combinada, por meio de operadores booleanos AND, registros contendo todos os termos, e OR, registros que contenham um dos termos (Picalho; Fadel; Gonçalves, 2023). Essa técnica permitiu localizar publicações pertinentes e relevantes, ampliando o conjunto de materiais consultados, possibilitando uma coleta de informações mais abrangente e consiste.

Em seguida, foi realizada uma visita prévia em uma empresa de pequeno porte, localizada na cidade de Macapá, estado do Amapá, para levantamento e diagnóstico do ambiente computacional, com o objetivo de identificar vulnerabilidades, falhas de segurança e limitações da infraestrutura existente. Nessa etapa foram analisados aspectos relacionados à tipologia da rede, controle de acesso, distribuição de serviços, gerenciamento de usuários e mecanismos de proteção disponíveis.

Após o diagnóstico, ocorreu a etapa de implantação do firewall PfSense, onde foi elaborada uma proposta de reestruturação da infraestrutura de rede, contemplando a definição da arquitetura lógica do ambiente, segmentação da rede, implementação de mecanismos de controle de acesso e adoção de boas práticas de segurança. Em seguida ocorreu a instalação e configuração do PfSense, incluindo a parametrização das interfaces de rede, definição de regras de filtragem de tráfego, configuração de acesso remoto seguro por VPN e instalação de pacotes complementares para monitoramento, geração de relatórios e controle da navegação web. Paralelamente, foram executadas ações de reorganização da infraestrutura tecnológica, incluindo a virtualização de servidores, implantação de serviços de diretório, DNS, DHCP, compartilhamento de arquivos e gerenciamento de usuários por meio de políticas de domínio.

Essas atividades tiveram como finalidade aumentar a disponibilidade, segurança e capacidade de gerenciamento dos recursos computacionais da organização.

Por fim, foi realizada a etapa de avaliação dos resultados, que ocorreu por meio da observação direta do funcionamento da solução implementada, análise dos registros gerados pelo firewall e verificação da capacidade do sistema em identificar e bloquear tentativas de acessos não autorizados. Além disso, foram realizados testes de funcionamento dos serviços implantados e treinamento dos colaboradores responsáveis pela administração do ambiente, possibilitando a transferência de conhecimento e continuidade operacional da solução.

A análise dos dados coletados foi realizada por meio da técnica de conteúdo, proposta por Bardin (2016), buscando interpretar informações obtidas no levantamento bibliográfico e nos resultados observados durante a implantação do firewall PfSense no ambiente corporativo. A análise das informações ocorreu por meio das etapas de pré-análise, com a sistematização e organização dos dados; agrupamento e categorização das ideias, com a exploração do material levantado; e inferências e conclusões, com o tratamento e interpretação das informações levantdas. Os conteúdos foram organizados em eixos temáticos relacionados à segurança da informação, firewalls, software livre e ao PfSense, posteriormente, foram interpretados de acordo com os objetivos da investigação e estabelecidas as conexões entre os diferentes autores, favorecendo análise e discussão robusta e aprofundada dos resultados.

4 RESULTADOS E DISCUSSÃO

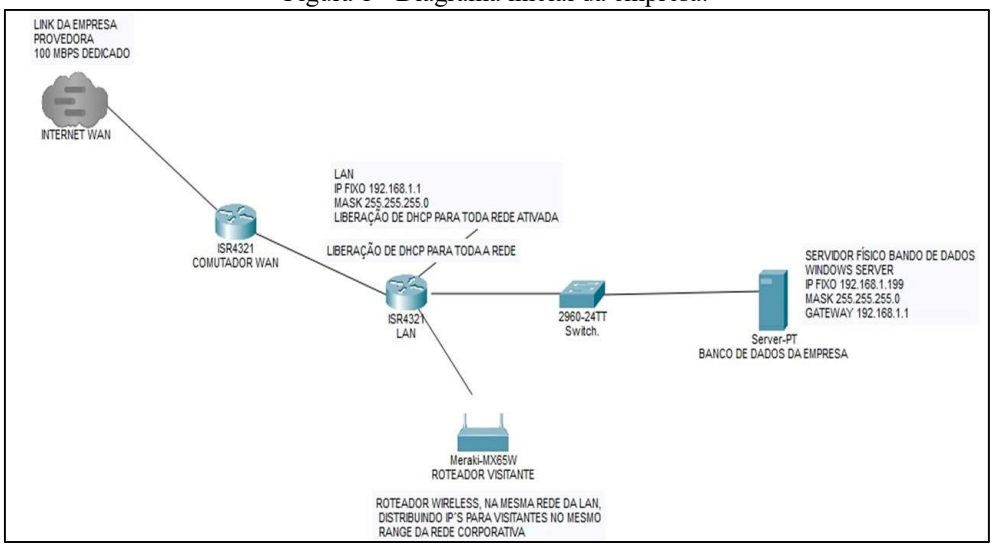
4.1 Caracterização do ambiente

A partir da análise dos resultados, identificou-se que a empresa selecionada para a aplicação da proposta apresentava vulnerabilidades relacionadas à segurança da informação e ausência de mecanismos adequados de controle de acesso à rede corporativa. A organização possuía infraestrutura tecnológica limitada (Figura 1) e dependia diretamente do roteador fornecido pela empresa responsável pelo link de internet.

Durante a análise do ambiente, foi verificado que a empresa provedora de internet possuía total controle sobre o roteador principal da organização, realizando inclusive alterações remotas relacionadas ao DHCP, abertura de portas e configurações da rede sem fio. Verificou-se ainda, que a rede wireless de visitantes utilizava o mesmo segmento da rede corporativa, permitindo que dispositivos externos pudessem tentar acessar recursos internos da organização.

Outro problema identificado diz respeito à ausência de mecanismos de autenticação centralizada e controle de permissões de usuários, dificultando a proteção de arquivos e compartilhamentos internos. Além disso, foi constatado que os colaboradores armazenavam documentos importantes localmente em suas máquinas, aumentando os riscos de perda de dados.

Figura 1 - Diagrama inicial da empresa.



Fonte: Elaborado pelo autor (2026).

A partir dos resultados, pode-se inferir que a segurança da informação se constitui como um dos pilares fundamentais para o funcionamento de organizações frente a intensificação da conectividade e exposição das redes corporativas a diferentes tipos de

ameaças cibernéticas. Conforme afirma Ferreira (2024), a proteção de ativos informacionais se apresenta como uma estratégia necessária para reduzir vulnerabilidades e garantir a continuidade das operações em empresas de todos os portes, destacando-se a adoção de mecanismos de controle de acesso e monitoramento de tráfego como investimento essencial para a proteção de dados corporativos.

Os princípios de confiabilidade, integridade e disponibilidade, esses elementos são basilares para a proteção das informações em ambientes computacionais. O estudo de Cicoli e Batistão (2025) sobre segurança em redes corporativas, evidencia que a ausência de mecanismos que garantem esses princípios resulta em perdas financeiras, interrupções operacionais e comprometimento da reputação organizacional. Além disso, Ferreira (2024), destaca que a segurança da informação não depende apenas da aquisição de recursos tecnológicos, mas também de políticas de proteção e acesso, procedimentos técnicos e operacionais e boas práticas de gestão. Essa percepção reforça a necessidade de uma abordagem mais integrada para que se possa efetivar a proteção das redes em ambientes corporativos.

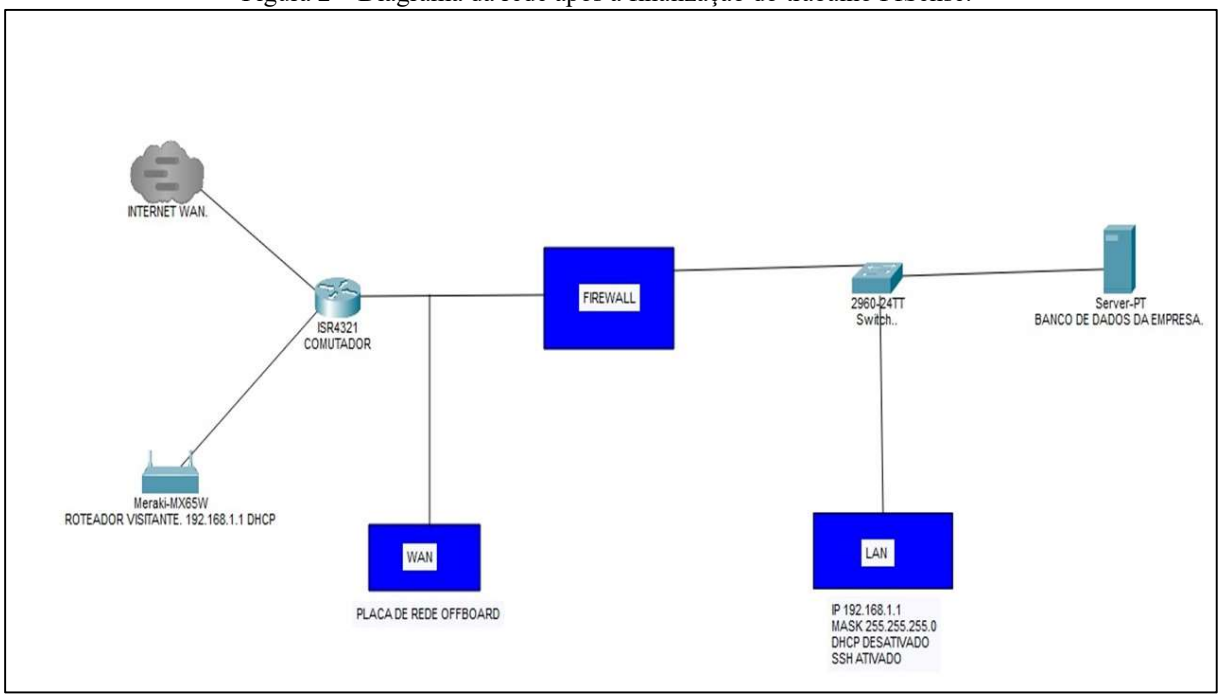
4.2 Planejamento da Infraestrutura e implantação do firewall PfSense

Após a análise do cenário inicial, foi elaborado um planejamento visando reestruturar parcialmente a infraestrutura tecnológica da organização, no intuito de fortalecer a segurança da informação, melhoria do gerenciamento da rede e aumento da disponibilidade dos serviços. O projeto contemplou a implantação do firewall PfSense como elemento central de proteção do ambiente computacional; a separação lógica entre rede corporativa e rede destinada a visitantes, reduzindo riscos de acessos indevidos aos recursos internos; a implementação de uma solução de VPN para acesso remoto seguro aos serviços da organização; a virtualização do servidor físico existente; a implantação de serviços de diretório para gerenciamento centralizado de usuários; a implementação de um servidor de arquivos; e a criação de políticas de autenticação e controle de acesso baseadas em perfis de usuários e grupos organizacionais.

A partir do projeto, foi elaborado um novo diagrama lógico da infraestrutura de rede, demonstrando a reorganização do ambiente após a implantação das melhorias propostas (Figura 2), onde o PfSense passou a atuar como ponto intermediário entre a internet e a rede corporativa, realizando a filtragem e o controle do tráfego de entrada e saíde. A interface WAN foi configurada para receber as conexões provenientes do provedor de internet, enquanto a interface LAN foi configurada com o endereço IP 192.168.1/24, tornando-se o gateway principal da rede interna. A tipologia que foi implementada previu a utilização de um

switch para a distribuição do tráfego aos dispositivos corporativos e ao servidor de banco de dados, que passou a operar em um segmento protegido pelo firewall. Paralelamente, a rede destinada aos visitantes foi isolada da infraestrutura corporativa por meio de roteador independente, utilizando faixa de endereçamento própria e sem acesso direto aos recursos internas da empresa.

Figura 2 – Diagrama da rede após a finalização do trabalho PfSense.



Fonte: Elaborado pelo autor (2026).

Além de representar a nova arquitetura da rede, o diagrama possibilitou documentar o fluxo de comunicação entre diferentes componentes da infraestrutura, evidenciando a segmentação dos ambientes, a centralização dos mecanismos de segurança no firewall e a adoção de uma estrutura mais adequada às boas práticas de segurança da informação. Essa reorganização permitiu aumentar o controle sobre os acessos à rede, reduzir vulnerabilidades existentes no ambiente original e criar condições para futuras expansões e aprimoramentos dos serviços de tecnologia da informação da empresa.

A implantação do PfSense seguiu um plano estruturado que contemplou atividades de instalação, configuração, testes, validação e capacitação dos usuários responsáveis pela administração da solução. Inicialmente, foi efetuada a instalação do sistema em equipamento dedicado, seguida da configuração das interfaces WAN e LAN, definição dos parâmetros básicos da rede, configuração do gateway padrão, serviços de DNS e demais recursos necessários ao funcionamento da infraestrutura de segurança. Posteriormente, foram

implementadas as políticas de controle e filtragem de tráfego, estabelecendo regras de acesso para monitorar e controlar as comunicações entre a rede interna e a internet. A configuração do firewall foi baseada no princípio da minimização de riscos, contemplando mecanismos de registro de eventos (logs), bloqueio de acessos não autorizados e monitoramento contínuo das conexões realizadas.

Também foram configuradas regras específicas para permitir apenas os serviços necessários ao funcionamento da organização, reduzindo a superfície de exposição a ameaças externas. Como parte das medidas de segurança que foram adotadas, foi implementada uma solução de acesso remoto seguro por meio do protocolo Open VPN no modelo Client-to-Site.

A autenticação dos usuários passou a ser realizada com base em certificados digitais individuais, aumentando a segurança das conexões remotas e reduzindo os riscos associados ao uso exclusivo de senhas. O processo envolveu a criação de usuários, geração e distribuição de certificados, exportação dos clientes VPN e realização de testes de conectividade em computadores e dispositivos móveis, garantindo acesso seguro aos recursos internos da organização mesmo fora do ambiente corporativo.

Para ampliar as funcionalidades nativas do PfSense, foram instalados e configurados pacotes complementares voltados à gestão, monitoramento e proteção da rede. Entre eles, destacam-se o Squid, utilizado como servidor proxy para o gerenciamento do acesso à internet; o SquidGuard, responsável pela filtragem de conteúdo e bloqueio de sites por categorias; o Lightsquid, empregado na geração de relatórios detalhados de navegação dos usuários; o OpenVPN Client Export, utilizado para simplificar a distribuição dos clientes VPN; o BandwidthD, responsável pelo monitoramento do consumo de banda e análise de tráfego por endereço IP; e o Cron, utilizado para automatização de tarefas administrativas e rotinas de manutenção.

A integração desses recursos proporcionou maior visibilidade sobre o comportamento da rede corporativa, permitindo identificar padrões de utilização, monitorar o consumo de recursos, controlar o acesso a conteúdo inadequado e registrar eventos relevantes para auditoria e investigação de incidentes. Além disso, os mecanismos de monitoramento implementados possibilitaram a geração de relatórios gerenciais e operacionais, contribuindo para uma administração mais eficiente da infraestrutura de rede e para o fortalecimento da política de segurança da informação da empresa.

As regras de segurança configuradas no PfSense tiveram como objetivo proteger a rede corporativa contra acessos externos não autorizados. Na interface WAN, foi liberada exclusivamente a porta UDP 1194 para conexões VPN autenticadas por certificados digitais,

enquanto todas as demais portas permanecem bloqueadas. Foram também configurados registros de logs para monitorar as tentativas de acesso e aplicada a política de bloqueio padrão (Clean-Up Rule), para bloquear automaticamente todo tráfego não autorizado.

Essas configurações permitiram reduzir a superfície de ataque da empresa e identificar diversas tentativas de conexão maliciosa provenientes da internet, todas bloqueadas pelo firewall. Na interface LAN, foi inicialmente adotada uma política permissiva, permitindo a comunicação dos dispositivos internos com a internet. Contudo, recomendou-se à empresa a implementação futura de regras mais restritivas, baseadas nos serviços efetivamente utilizados, visando fortalecer ainda mais a segurança da rede.

4.3 Resultados observados

Os resultados observados após a implantação demonstraram a capacidade do PfSense de detectar e bloquear tentativas de acesso indevido provenientes da Internet, evidenciando sua eficácia como ferramenta de proteção para ambientes corporativos de pequeno porte, onde foram observadas melhorias significativas na segurança e no gerenciamento da infraestrutura de rede da empresa. A análise dos registros gerados pelo sistema demonstrou a ocorrência de diversas tentativas de conexão provenientes de endereços IP externos direcionadas para portas frequentemente exploradas por agentes maliciosos em ataques cibernéticos (Figura 3).

Figura 3 - Registro de tentativas de conexões externas bloqueadas pelo firewall PfSense.

Firewall Logs

Act	Time	IF	Source	Destination
✖	Jun 4 19:18	WAN	104.247.75.190	[redacted]:23
✖	Jun 4 19:18	WAN	152.32.205.193	[redacted]:5681
✖	Jun 4 19:18	WAN	114.122.130.135	[redacted]
✖	Jun 4 19:18	WAN	114.122.130.135	[redacted]
✖	Jun 4 19:18	WAN	162.216.149.201	[redacted]:9719
✖	Jun 4 19:18	WAN	194.88.98.118	[redacted]:2052
✖	Jun 4 19:18	WAN	94.231.206.15	[redacted]:5432
✖	Jun 4 19:18	WAN	151.243.11.245	[redacted]:8080
✖	Jun 4 19:18	WAN	104.247.75.190	[redacted]:23
✖	Jun 4 19:18	WAN	66.132.172.127	[redacted]:32917

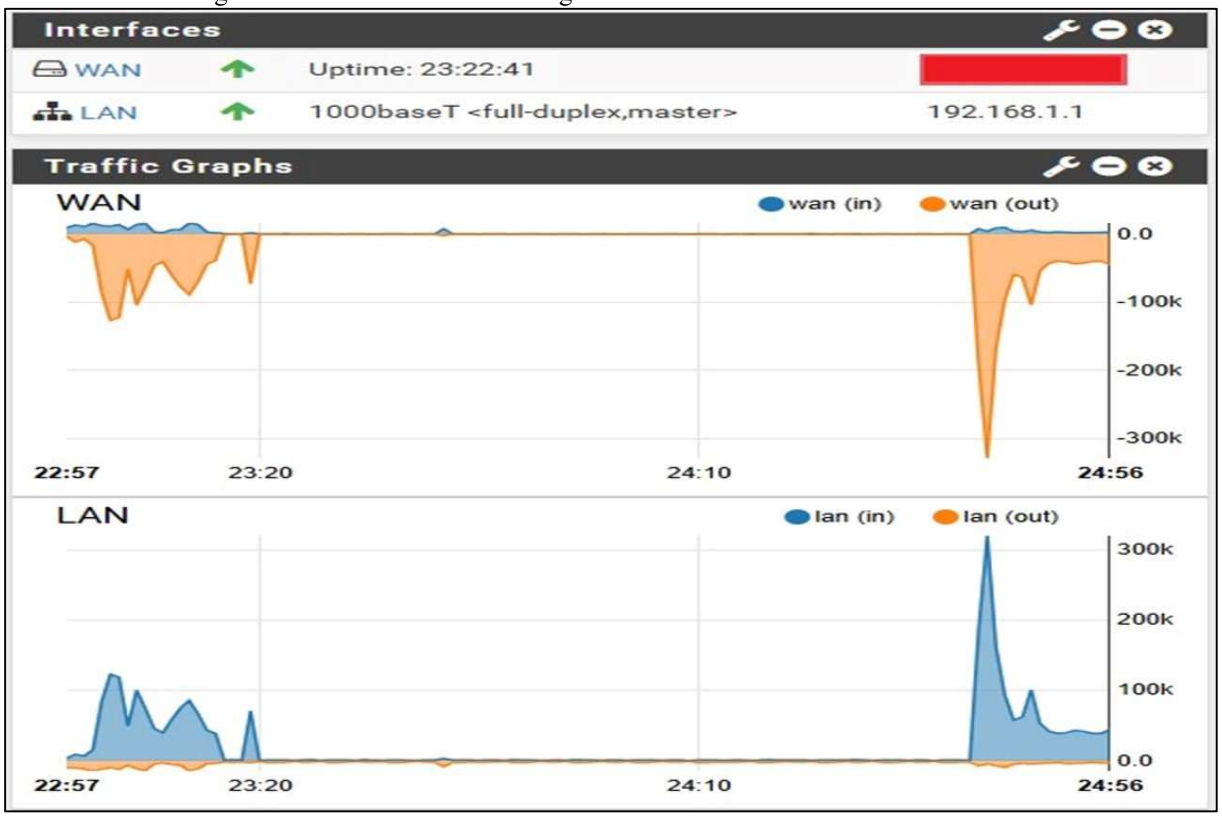
Fonte: Elaborado pelo autor (2026).

Conforme mostra a figura 3, foram registradas tentativas de acesso às portas 23 (Telnet), 5681, 8080 e outras portas de serviços, amplamente associadas a acessos não autorizados e à propagação de malware e ransomware. Todas as tentativas identificadas foram

bloqueadas pelas regras de filtragem configuradas no firewall. Esses registros evidenciam a importância da proteção perimetral, demonstrando que a organização estava constantemente exposta a tentativas automatizadas de varredura e exploração de vulnerabilidades.

Além da proteção perimetral, a solução implementada proporcionou maior controle sobre o tráfego de dados da rede, isolamento da rede destinada a visitantes, redução da exposição dos serviços internos à internet e disponibilização de acesso remoto seguro por meio de VPN (Figura 4). A reestruturação do ambiente também contribui para a centralização da autenticação de usuários, melhoria do gerenciamento de arquivos e recursos compartilhados e monitoramento contínuo das conexões realizadas na rede corporativa.

Figura 4 - Monitoramento do tráfego das interfaces WAN e LAN no PfSense.

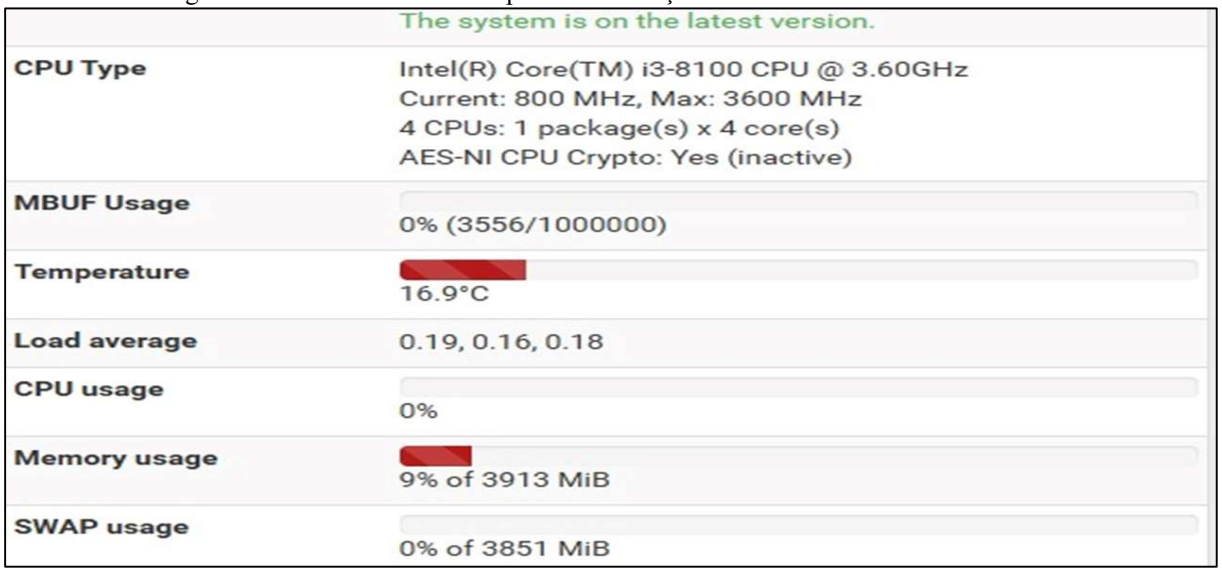


Fonte: Elaborado pelo autor (2026).

Conforme mostra a figura 4, a capacidade de monitoramento em tempo real do tráfego de rede é um dos benefícios oferecidos pelo PfSense, os gráficos que são disponibilizados permitem acompanhar o comportamento das interfaces WAN e LAN, possibilitando a identificação de picos de utilização, análise do consumo de banda e acompanhamento do fluxo de dados entre a internet e a rede corporativa. Essas informações são importantes para tomadas de decisões relacionadas à capacidade da infraestrutura e à detecção de comportamentos anômalos. Além dos aspectos relacionados à segurança, o monitoramento

dos recursos do equipamento demonstrou que firewall implantado operou com baixo consumo de processamento e memória durante o período analisado (Figura 5).

Figura 5 - Indicadores de desempenho e utilização de recursos do firewall PfSense.

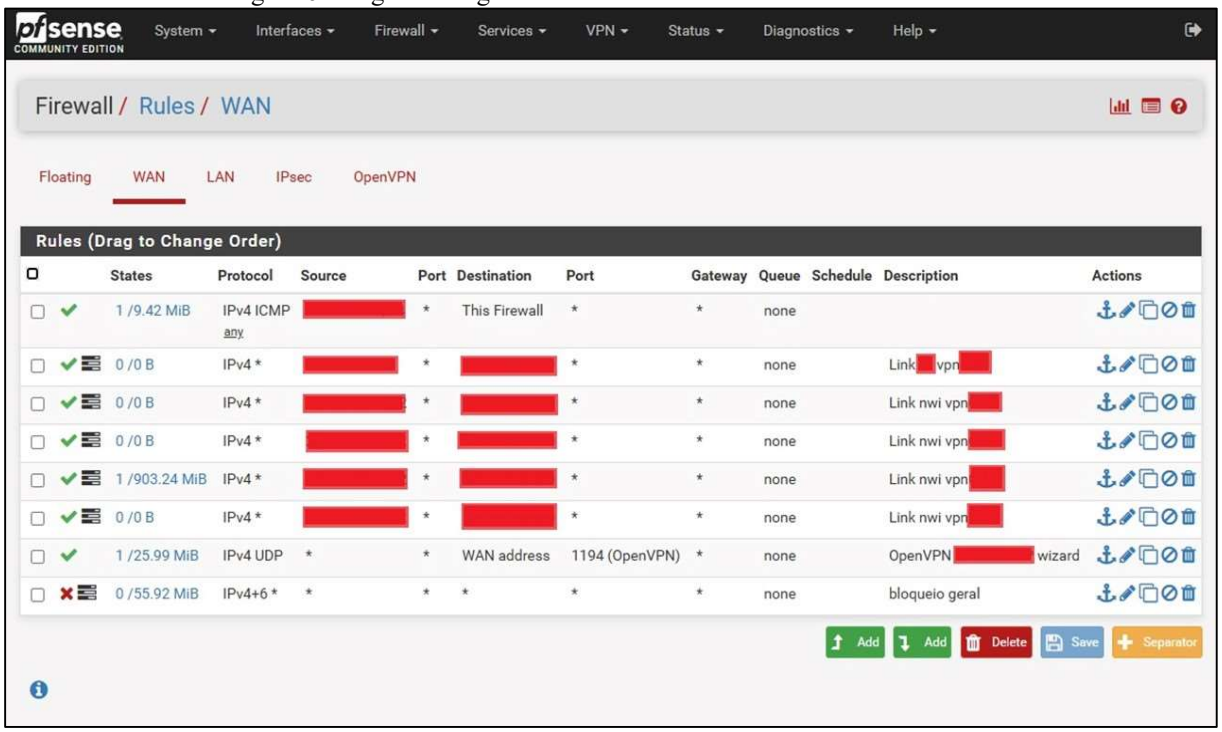


Fonte: Elaborado pelo autor (2026).

Conforme mostra a figura 5, a utilização da CPU permaneceu próxima de 0%, enquanto o consumo de memória manteve-se abaixo de 10%, evidenciando que a solução pode ser executada de forma eficiente em hardware de baixo custo. Esse resultado reforça a viabilidade do PfSense para pequenas organizações que necessitam implementar mecanismos avançados de segurança sem elevados investimentos em infraestrutura.

A figura 6 apresenta as principais regras configuradas na interface WAN do PfSense durante a implantação da solução de segurança da informação na empresa analisada, onde foi observada inicialmente uma regra ICMP utilizada para testes de conectividade e monitoramento da infraestrutura de rede. Em seguida, foram implementadas regras específicas de liberação para conexões autorizadas provenientes de endereços previamente definidos, restringindo acessos externos apenas para serviços necessários.

Figura 6 - Regras configuradas na interface WAN do firewall PfSense.

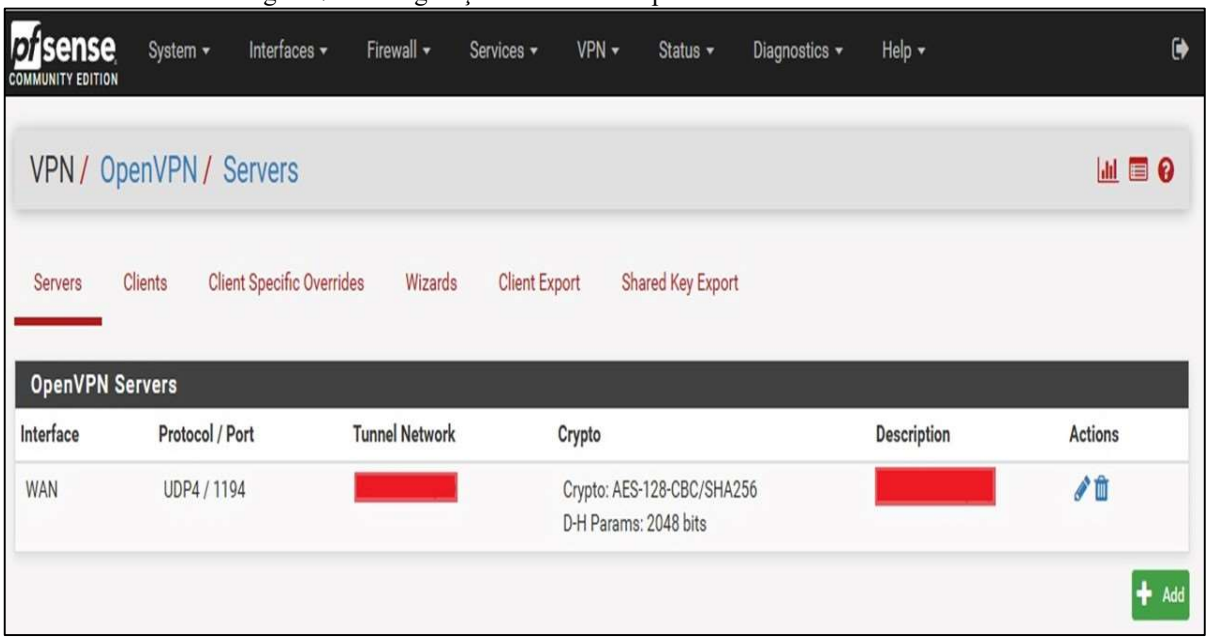


Fonte: Elaborado pelo autor (2026).

Conforme mostra a figura 6, foi também configurada uma regra destinada ao funcionamento do serviço OpenVPN utilizando a porta UDP 1194, permitindo acesso remoto seguro à rede corporativa por meio de conexões criptografadas e autenticação baseada em certificados digitais. Por fim, foi implementada uma regra geral de bloqueio geral, responsável por negar conexões externas não autorizadas. Essa abordagem segue o princípio "*deny all*", considerado uma boa prática em políticas de firewall, onde apenas serviços explicitamente autorizados permanecem acessíveis. As regras implementadas contribuíram para o controle do tráfego de rede, redução da superfície de ataque, proteção contra acessos indevidos, monitoramento de conexões externas, fortalecimento da segurança da informação da empresa.

No que diz respeito ao serviço OpenVPN, para sua configuração foi utilizado o protocolo UDP na porta 1194, padrão amplamente utilizado. Além disso, foram aplicados mecanismos criptográficos baseados em AES-128-CBC e autenticação SHA256, associados a parâmetros Diffie-Hellman de 2048 bits, visando garantir maior segurança na comunicação entre clientes remotos e a rede corporativa. A Figura 7 apresenta a configuração do servidor OpenVPN implementado no firewall PfSense para permitir acesso remoto seguro à rede corporativa da organização analisada.

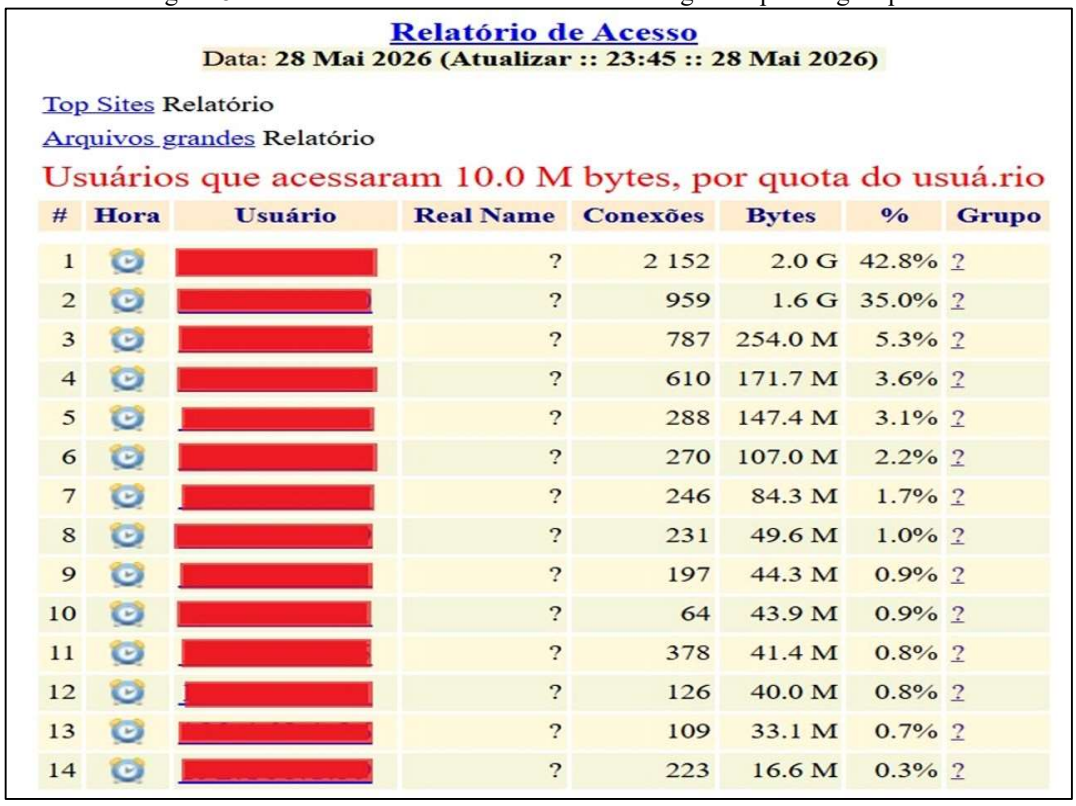
Figura 7 - Configuração do servidor OpenVPN no firewall PfSense.



Fonte: Elaborado pelo autor (2026).

A utilização da VPN possibilitou que usuários autorizados acessassem recursos internos da organização de forma segura por meio de conexões criptografadas, reduzindo riscos relacionados à exposição de serviços diretamente na internet. Em relação ao monitoramento de acessos, a figura 8 apresenta um relatório gerado pelo pacote Lightsquid integrado ao firewall PfSense após a implantação da solução de segurança na organização analisada. O relatório permitiu identificar os usuários com maior volume de tráfego na rede corporativa, apresentando informações relacionadas à quantidade de conexões realizadas, consumo de banda e percentual de utilização da rede.

Figura 8 - Relatório de monitoramento de acessos gerado pelo Lightsquid.



Relatório de Acesso

Data: **28 Mai 2026 (Atualizar :: 23:45 :: 28 Mai 2026)**

Top Sites Relatório

Arquivos grandes Relatório

Usuários que acessaram 10.0 M bytes, por quota do usuá.rio

#	Hora	Usuário	Real Name	Conexões	Bytes	%	Grupo
1		[redacted]	?	2 152	2.0 G	42.8%	?
2		[redacted]	?	959	1.6 G	35.0%	?
3		[redacted]	?	787	254.0 M	5.3%	?
4		[redacted]	?	610	171.7 M	3.6%	?
5		[redacted]	?	288	147.4 M	3.1%	?
6		[redacted]	?	270	107.0 M	2.2%	?
7		[redacted]	?	246	84.3 M	1.7%	?
8		[redacted]	?	231	49.6 M	1.0%	?
9		[redacted]	?	197	44.3 M	0.9%	?
10		[redacted]	?	64	43.9 M	0.9%	?
11		[redacted]	?	378	41.4 M	0.8%	?
12		[redacted]	?	126	40.0 M	0.8%	?
13		[redacted]	?	109	33.1 M	0.7%	?
14		[redacted]	?	223	16.6 M	0.3%	?

Fonte: Elaborado pelo autor (2026).

Esse tipo de monitoramento contribui para o gerenciamento da infraestrutura tecnológica da organização, possibilitando identificar padrões de utilização da internet, consumo excessivo de banda e possíveis comportamentos inadequados na rede corporativa. Além disso, os relatórios gerados auxiliam na implementação de políticas de controle de acesso e gestão de tráfego, fortalecendo os mecanismos de segurança e administração da rede.

Contudo, os resultados obtidos evidenciam que o PfSense se apresenta como uma solução eficiente e economicamente viável para organizações de pequeno porte, ofertando recursos avançados de segurança, monitoramento e controle de acesso sem a necessidade de investimentos elevados em equipamentos ou licenças proprietárias. Dessa forma, a ferramenta contribui para o fortalecimento da segurança da informação e para uma gestão mais segura e organizada da infraestrutura tecnológica da empresa.

4.4 Discussão dos resultados

Os resultados observados durante a implantação do PfSense corroboram com os estudos de Dourado (2022), Fachinelli e Ahlert (2014), Fontanelli (2018), Godoy (2016), Lopez (2020), Milani e Dian (2025), Neves, Machado e Centenaro (2014), especialmente no que se refere à importância dos firewalls como mecanismos de controle de acesso e proteção

contra ameaças externas. A atualização do PfSense demonstrou que soluções Open Source podem oferecer funcionalidades robustas de segurança, incluindo VPN, filtragem de tráfego, monitoramento e geração de relatórios, sem a necessidade de elevados investimentos financeiros.

Os autores consultados destacam que os firewalls atuam como barreiras de proteção entre redes internas e externas, controlando o tráfego de dados com base em regras e normas previamente definidas. Essa capacidade de filtragem permite restringir comunicações e acessos indevidos, bem como reduzir a superfície de exposição das organizações. Além disso, os estudos analisados demonstram que o firewall desempenha um papel importante na implementação de políticas de segurança e segmentação de redes. Dessa forma, os resultados encontrados indicam que a sua utilização é considerada uma das práticas mais eficazes para proteção das infraestruturas computacionais.

No que diz respeito à diz respeito à evolução tecnológica dos firewalls, os resultados alcançados coadunam com os estudos de Milani e Dian (2025) e Evangelista (2014), os autores demonstraram que as soluções atuais proporcionam recurso mais avançados do que os modelos tradicionais de filtragem de pacotes. Funcionalidades como inspeção de estado, análise de aplicações, monitoramento em tempo real e integração com sistemas de prevenção de intrusão ampliaram significativamente a capacidade de proteção dessas ferramentas. Essa evolução consolidou os firewalls como elementos centrais de estratégias contemporâneas de segurança da informação. Os autores ressaltam ainda que a combinação dessas funcionalidades contribui para uma resposta mais eficiente às ameaças atuais, tornando-os componentes indispensáveis das arquiteturas de segurança.

Em relação ao software livre e ao movimento open source, os resultados obtidos se aproximam dos estudos de Barbosa e Reis (2016), Biondo, Morcelli e Neitzke (2023), Nascimento (2023) e Rossi e Bochnia (2023), onde é evidenciado que essas iniciativas são essenciais para o desenvolvimento de tecnologias acessíveis e inovadoras. As literaturas analisadas apontam que a disponibilização do código-fonte promove transparência, colaboração e independência tecnológica, permitindo que comunidades de desenvolvedores contribuam para a evolução constante dos sistemas. Os estudos demonstram que muitas soluções open source apresentam níveis elevados de estabilidade, desempenho e segurança, contribuindo para sua adoção em ambientes corporativos, consolidando-se como uma alternativa às soluções proprietárias.

No que diz respeito às vantagens econômicas, os resultados alcançados corroboram com os estudos de Barbosa e Reis (2016), Evangelista (2014) e Nascimento (2023), onde

destacam que a ausência de custos de licenciamento representa um fator decisivo para organizações adotarem os softwares de código aberto, principalmente as que possuem recursos financeiros limitados. Os autores ressaltam que empresas de pequeno porte, instituições públicas e organizações em fins lucrativos podem implementar soluções tecnológicas robustas sem comprometer o orçamento, tendo em vista a redução de custos, flexibilidade de customização e independência de fornecedores são apontados como benefícios diretos proporcionados pelos softwares open source. Essas características tornam os ambientes tecnologicamente mais eficientes e sustentáveis, nesse sentido, as literaturas analisadas confirmam a sua relevância no cenário tecnológico atual das organizações.

Sobre a ferramenta PfSense, os resultados dos estudos de Dourado (2022), Godoy (2016), Lopez (2020) e Neves, Machado e Centenaro (2014), demonstram o seu reconhecimento como uma das principais soluções open source para segurança de redes, os autores apontam que o sistema reúne funcionalidades avançadas de firewall, roteamento, VPN, segmentação de rede e monitoramento de tráfego em uma única plataforma. Os autores destacam que a integração desses recursos permite que as organizações implementes políticas de segurança robustas utilizando infraestrutura de baixo custo, mas com elevado nível de estabilidade e confiabilidade, fatores que contribuem para sua ampla implementação em diferentes contextos organizacionais.

Lopez (2023) e Neves, Machado e Centenaro (2014) evidenciam que a flexibilidade é um dos aspectos vantajosos para implantação do PfSense, por ser baseado em software livre, o sistema pode ser executado em equipamentos convencionais, eliminando a necessidade de aquisição dispositivos especializados. De acordo com os autores, essa característica reduz os custos de implementação e manutenção, sendo um fator relevantes para pequenas empresas que possuem restrições orçamentárias e não conseguem ampliar investimentos em segurança da informação, sendo apontado como uma alternativa tecnicamente e economicamente viável e eficiente para proteção de redes corporativas.

Quanto aos recursos avançados disponibilizados pelo PfSense, Dourado (2022), Godoy (2016) destacam funcionalidades como VPN, VLAN, balanceamento de carga, alta disponibilidade e integração com sistemas de detecção de invasão ampliam a capacidade de segurança do ambiente. Os autores ressaltam que esses recursos permitem a implementação de estratégias de defesa compatíveis com as necessidades das organizações. A interface de gerenciamento baseada na web facilita a administração da ferramenta, reduzindo a complexidade operacional, além disso, a combinação entre funcionalidades avançadas somada

a facilidade de uso, se apresentam como diferencial do PfSense em relação às alternativas disponíveis.

Observa-se ainda nos estudos analisados, que o PfSense é apontado como uma ferramenta que contribui para o aumento da segurança e do controle de acessos em redes corporativas de pequeno porte, devido a sua capacidade de filtrar o tráfego, restringir conexões não autorizadas, monitoramento de atividades e segmentação de ambientes de rede. Esses fatores contribuem para o fortalecimento da proteção organizacional, demonstrando que sua implantação atende às necessidades técnicas e financeiras de pequenas empresas. Nesse sentido, a adoção do PfSense alinha-se às tendências tecnológicas atuais que proporcionam segurança para os ambientes digitais, contribuindo para a sua implantação e desenvolvimento de sistemas cada vez mais eficientes e seguros.

A partir dos resultados alcançados com a implantação do PfSense e com as literaturas analisadas, pode-se inferir que o PfSense se apresenta como uma alternativa capaz de proporcionar para as organizações o aprimoramento da sua infraestrutura de segurança. Os resultados desses estudos reforçam ainda a importância dos firewalls como mecanismos essenciais que promovem a proteção de redes e evidenciam o potencial das ferramentas open source para democratização do acesso às tecnologias de segurança. Desse modo, conclui-se que as contribuições do PfSense para o controle de acessos e proteção de redes corporativas atendem as necessidades e demandas relativas à segurança da informação com baixo custo de implantação, favorecendo a sua adoção em ambientes corporativos de pequeno porte.

5 CONSIDERAÇÕES FINAIS

A partir dos resultados alcançados, conclui-se que a utilização do firewall PfSense contribui para o fortalecimento da segurança e do controle de acesso na rede corporativa analisada. A implantação prática realizada durante o estudo de caso demonstrou que soluções Open Source podem atender de forma eficiente às demandas de segurança da informação em organizações de pequeno porte. Os resultados observados evidenciaram que o firewall foi capaz de bloquear tentativas de acessos indevidos, segmentar adequadamente os ambientes de rede, implementar mecanismos seguros de acesso remoto e ampliar a capacidade de monitoramento da infraestrutura tecnológica da organização.

Além disso, verificou-se que a utilização do PfSense em conjunto com serviços complementares, como VPN, proxy e monitoramento de tráfego, possibilitou a implementação de uma infraestrutura mais segura e organizada sem elevados custos financeiros. Outro aspecto relevante refere-se à viabilidade da utilização de hardware de baixo custo associado a soluções Open Source para implementação de mecanismos avançados de proteção de redes corporativas, tornando essa alternativa acessível para pequenas empresas que possuem limitações orçamentárias.

Considera-se ainda, que as soluções de código aberto, consolidadas como alternativas estratégicas para a modernização das infraestruturas de tecnologia da informação, reúnem um conjunto abrangente de funcionalidades voltadas à segurança de redes. Dentre elas, destaca-se as funcionalidades do Pfsense, que apresentam características que possibilitam a implementação de políticas robustas de segurança mesmo em ambientes com limitações orçamentárias. Além disso, sua compatibilidade com hardware de baixo custo amplia sua acessibilidade e reforça sua viabilidade para pequenas empresas que necessitam fortalecer seus mecanismos de proteção digital.

Por fim, considera-se que os objetivos propostos foram alcançados satisfatoriamente, uma vez que foi possível analisar, implementar e observar na prática as contribuições do firewall PfSense para a segurança da informação em um ambiente corporativo real. Sugere-se que trabalhos futuros realizem análises comparativas entre diferentes soluções de firewall, bem como estudos voltados à implementação de mecanismos adicionais de detecção e prevenção de intrusão em ambientes corporativos. Dessa maneira, espera-se que este trabalho sirva como referência para estudantes, pesquisadores e profissionais interessados na utilização de tecnologias livres voltadas à segurança da informação.

REFERÊNCIAS

ALVES, M. R.; SOUZA, L. A. Segmentação de redes com VLANs: fundamentos, práticas e desafios. **Revista Brasileira de Segurança da Informação**, v. 12, n. 3, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001**: segurança da informação, segurança cibernética e proteção da privacidade — Sistemas de gestão da segurança da informação — Requisitos. 3 ed. Rio de Janeiro: ABNT, 2022.

BARBOSA, T. S.; REIS, F. A. O uso de ferramentas open source para aplicações de segurança em redes corporativas: um estudo baseado em firewalls. **Revista Saber Digital**, v.5. n.1, 2012.

BARDIN, L. **Análise de Conteúdo**. São Paulo: Edições 70, 2016.

BIONDO, U. R. L.; MORCELLI, D. B.; NEITZKE, G. H. Tecnologias Open-source na Base Nacional Comum Curricular de Ciência de Computação para a Educação Básica. In: Congresso Latino-Americano de Software Livre e Tecnologias Abertas, 20, 2023. **Anais** do 20º Congresso Latino-Americano de Software Livre e Tecnologias Abertas, Foz do Iguaçu, Paraná, 2023.

CICOLI, C. D. A.; BATISTÃO, E. **Segurança em redes corporativas**. Interface Tecnológica, Taquaritinga, SP, v. 22, n. 2, 2025.

DOURADO, R. S. **Um estudo dos *softwares Endian firewall* e *Pfsense firewall***. Monografia (Graduação). Pontífica Universidade Católica de Goiás, Goiânia, GO, 2022.

EVANGELISTA, R. O. Movimento software livre do Brasil: política, trabalho e hacking. **Horizontes Antropológicos**, Porto Alegre, ano 20, n. 41, 2014.

FACHINELLI, M.; AHLERT, E. M. Firewall de próxima geração – Fortinet. **Revista Destaques Acadêmicos**, v. 11, n. 14, Lajeado, RS, 2019.

FERREIRA, D. **Segurança de rede, defesa cibernética e operações**. 1 ed. Lisboa: Editora de Informática, 2024.

FONTANETTI, L. M. **Segurança da Informação em Redes Empresariais com Firewall Netfilter**. Monografia (Graduação), Faculdade de Tecnologia de Americana, Centro Estadual de Educação Tecnológica Paula Souza, Curso Superior de Tecnologia em Segurança da Informação, São Paulo, SP, 2018. 36f.

GODOY, H. A. **Alta disponibilidade em firewall utilizando o Pfsense**. Cinfotec Unicamp, 5 ed., Campinas, SP, 2016.

LOPEZ, P. A. V. P. **Implantação e análise da ferramenta pfsense como Firewall**. Monografia (Especialização), Universidade Tecnológica Federal do Paraná, Curso de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Curitiba, PR, 2020.

MARCONI, M. A.; LAKATOS, E. M. **Metodologia científica**. 8. ed. São Paulo: Atlas, 2022.

MILANI, L. E. A. B.; DIAN, M. O. Evolução dos firewalls e o uso de next-generation firewall (NGFW). **Interface tecnológica**, v. 22, n. 2, Taquaritinga, SP, 2025.

NASCIMENTO, E. M. **Software livre e de código aberto na gestão pública**. Monografia (Especialização), Curso de Especialização em Administração Pública, Planejamento e Gestão Governamental, Escola de Governo Professor Paulo Neves de Carvalho, Fundação João Pinheiro, Vitória, ES, 2023.

NEVES, F. C.; MACHADO, L. A.; CENTENARO, R. F. **Implantação de Firewall PfSense**. Monografia (Graduação). Universidade Tecnológica Federal do Paraná, Departamento Acadêmico de Eletrônica, Curso Superior de Tecnologia em Sistemas de Telecomunicações, Curitiba, PR, 2014. 67f.

PICALHO, A. C.; FADEL, L. M.; GONÇALVES, A. L. **Expressões de busca e o uso de diferentes operadores avançados de pesquisa em um mecanismo de busca**. Texto livre, Belo Horizonte, v. 16, e47531, 2023.

ROSSI, G.; BOCHNIA, L. Chamando cada coisa pelo nome correto: as diferenças entre o Software Livre e o Código Aberto. In: Congresso Latino-Americano de Software Livre e Tecnologias Abertas, 21, 2024. **Anais** do 21º Congresso Latino-Americano de Software Livre e Tecnologias Abertas, Foz do Iguaçu, Paraná, 2023.

SILVA, A. C. Classificação metodológica das pesquisas científicas. In: Congresso Nacional de Pesquisas e Práticas em Educação, online, 2024. **Anais** do Congresso Nacional de Pesquisas e Práticas em Educação, v.2, n.1, 2024.