XXI Escola Regional de Redes de Computadores (ERRC). DOI: 10.5753/errc.2024.4557

ARTIGO CURTO/SHORT PAPER

Estudo Comparativo de Firewalls de Código Aberto Baseados em FreeBSD: pfSense vs. OPNsense

A Comparative Study of Open Source Firewalls Based on FreeBSD: pfSense vs. OPNsense

Emanuel de Franceschi Vieira Vieira • emanuel.franceschi@acad.ufsm.br
Universidade Federal de Santa Maria (UFSM)
Emerson Wendler • emerson.wendler@redes.ufsm.br
Universidade Federal de Santa Maria (UFSM)
Tiago Antonio Rizzetti • tiago.rizzetti@ufsm.br
Universidade Federal de Santa Maria (UFSM)
Renato Preigschadt De Azevedo • renato@redes.ufsm.br
Universidade Federal de Santa Maria (UFSM)

RESUMO. Este artigo apresenta uma análise comparativa preliminar entre dois *firewalls* de código aberto baseados em FreeBSD: pfSense e OPNsense. Ambas as ferramentas são amplamente utilizadas para controle de tráfego e segurança de redes, mas apresentam diferenças significativas em termos de desempenho, consumo de recursos e usabilidade. O estudo foi conduzido em um ambiente real com aproximadamente 500 dispositivos conectados, com foco inicial no consumo de processamento e memória de cada *firewall*. Resultados preliminares indicam diferenças significativas entre as soluções em relação ao uso de recursos. O objetivo final é identificar qual opção é mais eficiente para ambientes corporativos e educacionais que buscam uma solução de *firewall* de código aberto. Os próximos passos incluem testes mais abrangentes para avaliar latência, perda de pacotes e largura de banda.

ABSTRACT. This paper presents a preliminary comparative analysis between two open-source firewalls based on FreeBSD: pfSense and OPNsense. Both tools are widely used for traffic control and network security but differ significantly in performance, resource consumption, and usability. The study was conducted in a real environment with approximately 500 connected devices, initially focusing on each firewall's memory and processing consumption. Preliminary results indicate significant differences between the solutions in terms of resource usage. The ultimate goal is to identify which option is more efficient for corporate and educational environments seeking an open-source firewall solution. Future steps include more comprehensive tests to evaluate latency, packet loss, and bandwidth.

PALAVRAS-CHAVE: Análise de Desempenho • Firewall • FreeBSD • OPNsense • pfSense
KEYWORDS: Performance Analysis • Firewall • FreeBSD • OPNsense • pfSense

1 Introdução

O *firewall* atua como um escudo entre a rede interna e externa, regulando o tráfego entre sub-redes e permitindo autorizar, bloquear e registrar atividades, oferecendo maior controle da rede [1, 2]. A adoção de *firewalls* de código aberto tem se tornado cada vez mais atraente devido à forte colaboração da comunidade e ao ritmo constante de atualizações [3]. Entre os *firewalls* de código aberto baseados em FreeBSD, destacam-se o pfSense e o OPNsense, que derivam do m0n0wall, *firewall* lançado em 2003. O pfSense surgiu em 2004 como uma bifurcação do m0n0wall e, em 2015, o OPNsense foi criado a partir do pfSense. Embora possuam poucas linhas de código em comum, ambos competem pela confiança dos usuários, cada um com suas próprias vantagens [4].

Este estudo tem como objetivo realizar uma comparação entre os *firewalls* de código aberto pfSense e OPNsense, implementados em um ambiente real com uma grande quantidade de dispositivos conectados. A análise abrange não apenas o desempenho geral de cada solução, mas também aspectos específicos como consumo de memória, eficiência no processamento de dados, facilidade de configuração e administração no ponto de vista do responsável pela infraestrutura. Além disso, serão realizados testes de Qualidade de Serviço (QoS) para verificar a capacidade de gerenciamento de tráfego. O foco principal é analisar e identificar qual dessas soluções oferece o melhor desempenho e atende de maneira mais eficiente às necessidades de organizações públicas ou privadas que buscam uma alternativa de *firewall* de código aberto.

O restante do artigo está organizado da seguinte forma: Na Seção 2, são apresentados os trabalhos relacionados, a fim de fornecer um comparativo com os estudos existentes na literatura. A Seção 3 descreve a metodologia e desenvolvimento utilizada para a realização deste trabalho. Na Seção 4 são apresentados os resultados parciais obtidos durante a pesquisa. Por fim, a Seção 5 apresenta as considerações finais e os trabalhos futuros.

2 Trabalhos Relacionados

Diversos estudos têm comparado *firewalls* baseados em *software* livre, especialmente pfSense e OPNsense, em termos de desempenho, consumo de recursos e segurança. O trabalho de [5] avaliou o desempenho de ambos os *firewalls*, focando no consumo de recursos de *hardware* e funcionalidades de segurança. Constatou-se que o pfSense requer, no mínimo, 1GB de RAM, enquanto o OPNsense precisa de 2GB. Utilizando a ferramenta *iperf3* para testes de tráfego de rede, com 45 minutos de duração para cada *firewall*, observou-se que o pfSense apresentou maior velocidade de envio e recepção de pacotes, além de uma menor taxa de perda de pacotes em comparação ao OPNsense. No entanto, o OPNsense demonstrou um consumo de recursos de *hardware* maior, particularmente em termos de CPU e memória RAM.

O estudo de [6] destacou que o sistema operacional FreeBSD, base de ambos os firewalls, é reconhecido por sua confiabilidade, estabilidade, portabilidade de *hardware* e suporte eficiente a funcionalidades de rede. Em termos de segurança, [7] conduziu uma comparação entre pfSense e OPNsense, testando suas capacidades de resposta a ataques como varredura de portas, *ping* da morte e força bruta. Embora ambos os *firewalls* tenham bloqueado a varredura de portas com sucesso, apenas o pfSense foi eficaz na prevenção de ataques de força bruta, indicando uma maior robustez.

A pesquisa realizada por [8] destaca que o consumo de recursos, como CPU e memória, varia significativamente entre as soluções de segurança pfSense e OPNsense, especialmente ao ativar funcionalidades como NAT e proxy. O pfSense demonstrou um consumo de CPU em torno de 12% e uso de memória média de 29%, se mostrando mais eficiente. Por outro lado, o OPNsense apresentou um consumo de memória superior, com média de 49%, quase o dobro do uso do pfSense, além de maior impacto na CPU. Ambas as soluções deste trabalho contam com documentação clara e detalhada, incluindo guias passo a passo que facilitam a instalação, configuração e ativação de novos recursos UTM.

3 Metodologia e desenvolvimento

Este estudo realiza uma análise comparativa dos *firewalls* pfSense e OPNsense em um ambiente real de uma instituição federal de ensino, com cerca de 500 dispositivos conectados. A pesquisa se diferencia dos trabalhos relacionados por utilizar um cenário real, o que proporciona resultados mais precisos sobre o desempenho de cada *firewall*. A rede está segmentada em sub-redes organizadas por VLANs, permitindo configurações flexíveis e políticas de segurança específicas.

O processo de configuração foi dividido em duas etapas. A primeira consiste na implementação do pfSense em parte da rede, com uma migração gradual para minimizar impactos. Após a configuração inicial do pfSense, incluindo VLANs, regras de *firewall*, NAT e serviços como DHCP, o sistema foi expandido para toda a infraestrutura. Na segunda etapa, o OPNsense foi instalado, replicando a mesma configuração e regras do pfSense, assegurando uma comparação justa entre os dois *firewalls*.

Os testes foram realizados em um ambiente virtualizado utilizando o XCP-ng, configurado em um único *hardware* físico. As máquinas virtuais foram configuradas com processadores de 16 núcleos e 4 GiB de memória RAM cada. Esse ambiente permitiu a simulação de diferentes cenários de uso, possibilitando a avaliação do comportamento de ambos os *firewalls* em uma infraestrutura com diversas VLANs e alto volume de tráfego. Os dados sobre consumo de memória e processamento foram coletados ao longo de sete dias diretamente no XCP-ng, permitindo uma análise detalhada do uso de recursos por cada *firewall*. No entanto, foi necessário observar algumas limitações do XCP-ng em relação à configuração de VLANs e ao uso de múltiplas interfaces de rede, conforme discutido na Seção 4.

4 Resultados parciais

Até o momento, os *firewalls* pfSense e OPNsense foram implementados na rede da instituição, e as primeiras métricas referentes ao consumo de memória e processamento foram coletadas. Foram realizados testes em dois cenários distintos: inicialmente com os *firewalls* isolados, ou seja, apenas instalados nas máquinas, sem a rede ativa, e, em seguida, com ambos em operação, gerenciando todo o tráfego da rede.

A Figura 1 apresenta o consumo de memória em Gibibytes entre o OPNsense e o pfSense, em dois cenários (isolado e em operação). É possível observar que o OPNsense consome significativamente mais memória em comparação ao pfSense, tanto no estado isolado quanto em operação. Quando isolado, o OPNsense utiliza apro-

ximadamente 1,7 GiB, enquanto o pfSense utiliza menos de 1 GiB. Já em operação, o consumo de memória do OPNsense aumenta para mais de 2 GiB, enquanto o pfSense se mantém abaixo de 1 GiB. Esse padrão indica que o OPNsense tem uma maior demanda de memória em ambos os cenários.

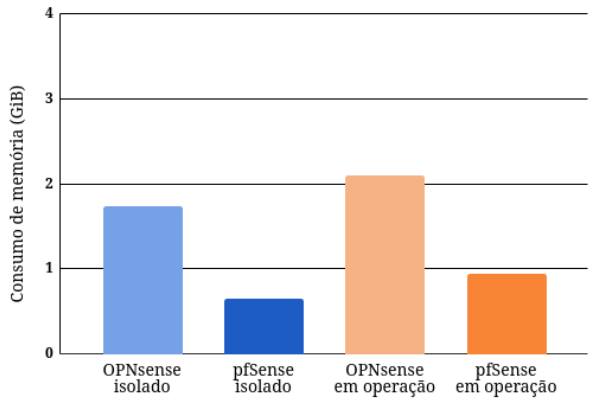

Figura 1. Média do consumo de memória.

Já o grafico, ilustrado na Figura 2, apresenta a porcentagem de consumo de processamento. No estado isolado, ambos os *firewalls* consomem pouca CPU, com o OPNsense e o pfSense mantendo-se abaixo de 5%. No entanto, em operação, há um aumento considerável no consumo de CPU de ambas as ferramentas, sendo que o pfSense atinge um consumo ligeiramente superior ao OPNsense. O pfSense utiliza aproximadamente 51% da CPU em operação, enquanto o OPNsense fica um pouco abaixo, em torno de 42%. Isso sugere que, embora o OPNsense consuma mais memória, o pfSense tende a exigir mais recursos de processamento durante a operação completa da rede.

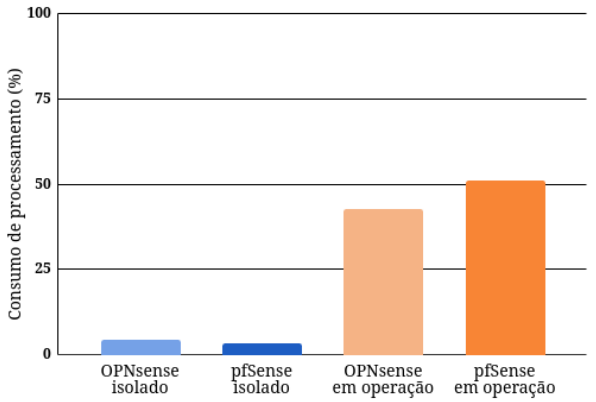

Figura 2. Média do consumo de processamento.

Um ponto importante a ser destacado durante a fase de testes foi a identificação de um problema relacionado à utilização do virtualizador XCP-ng em conjunto com os *firewalls* pfSense e OPNsense, especificamente ao configurar VLANs dentro do *firewall*. As interfaces VLAN criadas apresentavam uma Unidade Máxima de Transmissão (MTU) de 1496 *bytes*, o que resultava na impossibilidade de acessar determinados sites importantes, como páginas governamentais, na rede da instituição. Esse problema foi resolvido de duas maneiras: a primeira solução consistiu em aumentar a MTU da interface de chegada no servidor para 1504 *bytes* e, em seguida, implementar um *script* nos *firewalls* para ajustar a MTU das interfaces VLAN para 1500 *bytes*. Essa abordagem corrigiu o problema de conectividade. A segunda alternativa seria a criação de VLANs fora do *firewall*, mas o XCP-ng limita o número de interfaces de rede associadas a cada máquina virtual a 6, o que pode ser insuficiente em redes com múltiplas segmentações. Em cenários que exigem a criação de várias VLANs dentro do *firewall*, essa limitação pode gerar dificuldades operacionais adicionais.

5 Considerações finais e trabalhos futuros

Com base nos resultados preliminares deste estudo, é possível observar que tanto o pfSense quanto o OPNsense apresentam comportamentos distintos no gerenciamento de recursos, mas ainda não é possível concluir qual deles é mais eficiente de forma definitiva. O pfSense mostrou um menor consumo de memória, enquanto o OPNsense apresentou uma utilização mais eficiente da CPU durante a operação. A escolha entre as duas soluções dependerá de análises mais abrangentes e das necessidades específicas do ambiente, como a disponibilidade de recursos e a demanda por processamento. Os testes de Qualidade de Serviço (QoS) ainda não foram realizados. Testes futuros, envolvendo métricas como latência, perda de pacotes e largura de banda, irão permitir uma avaliação mais completa e ajudarão a identificar qual *firewall* é mais adequado para determinado cenário.

Este estudo se diferencia dos demais da literatura por analisar pfSense e OPNsense em um ambiente real com cerca de 500 dispositivos conectados, enquanto a maioria dos estudos usa ambientes simulados ou de menor escala. Além disso, o presente trabalho considera também aspectos operacionais de configuração e administração, relevantes para administradores de infraestrutura. Diferente de estudos anteriores, a proposta atende um cenário mais amplo, envolvendo desafios de performance e conectividade no uso combinado do XCP-ng e *firewalls* com múltiplas VLANs, oferecendo subsídios para decisões em infraestrutura de redes com demandas similares.

Agradecimentos

O presente trabalho foi realizado com apoio da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES.

Referências

1 Moraes, A. F. de. *Segurança em Redes - Fundamentos*. SRV Editora LTDA, 2010. E-book. ISBN 9788536522081. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788536522081/. Acesso em: 6 jun. 2024.

2 Fachinelli, M.; Ahlert, E. M. Firewall de próxima geração-fortinet. *Revista Destaques Acadêmicos*, v. 11, n. 4, 2019.

3 Zenarmor. *Best Firewalls for Schools*. Mai. 2034. Disponível em: https://www.zenarmor.com/docs/network-security-tutorials/best-firewalls-for-schools. Acesso em: 25 set. 2024.

4 Stubbig, M. *Practical OPNsense: Building Enterprise Firewalls with Open Source*. BoD–Books on Demand, 2023.

5 Llanes, R. P. Performance Evaluation of Free Software Based Firewalls. *Revista Digital Novasinergia*, Universidad Nacional de Chimborazo, v. 5, p. 31–42, 2022. Disponível em: https://orcid.org/0000-0001-7288-6224.

6 Zajeganović, M. *et al.* pfSense Router and Firewall Software. *In*: SINGIDUNUM UNIVERSITY. SINTEZA 2023-International Scientific Conference on Information Technology, Computer Science, and Data Science. 2023. P. 132–137.

7 Kiratsata, H. J. *et al.* Behaviour analysis of open-source firewalls under security crisis. *In*: IEEE. 2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET). 2022. P. 105–109.

8 Silva, R. F. da. *Análise comparativa de soluções de Open Source para cibersegurança por monitorização de tráfico de rede*. 2020. Diss. (Mestrado) – Instituto Politecnico de Beja (Portugal).