Firewalls de Próxima Geração (NGFW): Funcionalidades, Aplicações e Vulnerabilidades

Tiago W. Morais[1], Nícolas N. Faria[1], Silvio E. Quincozes[1,2], Diego Kreutz[1]
Juliano F. Kazienko[3], Vagner E. Quincozes[4] e Mário C. Peixoto[5]

[1]LEA, PPGES — Universidade Federal do Pampa (UNIPAMPA) – Alegrete, Brasil.

[2]FACOM — Universidade Federal de Uberlândia (UFU) – Uberlândia, Brasil.

[3]CTISM – Universidade Federal de Santa Maria (UFSM) – Santa Maria, Brasil.

[4]IC – Universidade Federal Fluminense (UFF) – Niterói, Brasil.

[5]TIS TECH – Luanda, Angola.

{tiagomorais, nicolasfaria}.aluno@unipampa.edu.br

{silvioquincozes, diegokreutz}@unipampa.edu.br

kazienko@redes.ufsm.br,vequincozes@midiacom.uff.br,

pintaudi@gmail.com

Resumo. *Os Firewalls de Próxima Geração (NGFWs) surgiram como uma ferramenta em resposta ao aumento dos crimes cibernéticos, integrando Inteligência Artificial (IA) e Aprendizado de Máquina (AM) em suas funcionalidades. Este estudo identifica e analisa os NGFWs de última geração e alto desempenho dos principais fabricantes, incluindo Check Point, Cisco, Fortinet, Huawei, Juniper, Palo Alto, SonicWall e Sophos. A principal contribuição deste trabalho é uma análise abrangente dos aspectos técnicos, mercadológicos e da avaliação dos usuários, a partir da comparação de oito ferramentas avançadas de NGFW. Foram mapeadas suas principais características, expectativas dos usuários, desafios e vulnerabilidades, fornecendo uma visão detalhada dessas soluções.*

1. Introdução

A pandemia de COVID-19 impulsionou o comércio eletrônico, movimentando cerca de 450 bilhões de reais no Brasil em três anos [Castro 2023]. Esse crescimento causou um aumento nos crimes cibernéticos, com 31,5 bilhões de tentativas de ataques no Brasil no primeiro semestre de 2022. Globalmente, estima-se que fraudes no comércio eletrônico representem 22% do capital movimentado [Solution 2023]. Fraudes comuns incluem *phishing*, *pharming*, fraudes de pagamento, roubo de cartões de crédito e cancelamento de negociações, com lojas online sendo os alvos principais [Santos and Nunes 2023].

Os NGFWs representam uma evolução significativa em relação aos *firewalls* tradicionais, oferecendo uma proteção mais robusta e abrangente contra ameaças cibernéticas emergentes [Liang and Kim 2022]. Além das funcionalidades tradicionais dos *firewalls*, os NGFWs são capazes de analisar atividades suspeitas na rede, desde a camada 2 até a camada 7 do modelo OSI. Essa análise avançada permite uma detecção mais precisa e

uma resposta rápida às ameaças [Neupane et al. 2018]. Existem diversos estudos que analisam e comparam NGFWs [NSSLabs 2014, Elnerud 2017, Malmgren and Persson 2016, Keary 2024, Nomios 2024, eSecurity 2024, Faizan et al. 2019], mas a maioria foca em um subconjunto limitado de NGFWs (*e.g.*, 2 a 4) e se restringe a descrever características gerais, vantagens, desvantagens e preços.

Este trabalho tem como principal objetivo identificar e analisar os NGFWs de última geração e alto desempenho dos principais fabricantes do mercado, incluindo Check Point Quantum Force 29200 [Point 2024a], Cisco Firepower 9300 [Cisco 2024], Fortinet FortiGate FG-7121F [Fortinet 2024], Huawei USG12008 [Huawei 2024], Juniper SRX5800 [Juniper 2024], Palo Alto PA-7500 [Alto 2024], SonicWall Supermassive-9800 [SonicWall 2024] e Sophos XGS 8500K [Sophos 2024]. O principal resultado é uma análise abrangente que considera aspectos técnicos, mercadológicos e dificuldades de uso e implementação desses dispositivos.

2. Trabalhos Relacionados

Existem diversos trabalhos que analisam e comparam NGFWs sob diferentes aspectos, como tipos de características, desempenho e proteção contra técnicas de evasão [Elnerud 2017, NSSLabs 2014, Keary 2024, Nomios 2024, Point 2024b, eSecurity 2024, Faizan et al. 2019, Malmgren and Persson 2016]. A maioria destes trabalhos comparava pontualmente duas ou três soluções (*e.g.*, Juniper SRX-1500 versus Palo Alto Networks PA-3020), observando aspectos como recursos disponíveis, usabilidade, quantidade de conexões suportadas e preço. Ademais, as análises desses trabalhos são limitadas ao escopo das redes corporativas de pequeno e médio porte. A Tabela 1 apresenta um resumo da ideia central dos trabalhos relacionados.

	Dominio de aplicação	**Aspectos analisados**	**Conclusões**
[NSSLabs 2014]	Redes de todos os tamanhos	Características e aplicações	Mostra o NGFW mais eficiente entre doze soluções
[Malmgren and Persson 2016]	Redes pequenas	Características, aplicações e preço	Palo Alto possui melhor visibilidade e desempenho
[Elnerud 2017]	Redes virtuais	Características, aplicações e preço	*Features* adicionais dimunuem o throughput
[Faizan et al. 2019]	Borda e data-center	Características, aplicações e preço	Cisco possui melhor visibilidade, Fortinet melhor desempenho
[Keary 2024]	Em nuvem	Características e preço	Check Point é melhor, baseado em features e vulnerabilidades
[Nomios 2024]	Data-centers	Características e preço	Apresenta os melhores NGFWs, baseado em algum ponto forte
[eSecurity 2024]	Indústria e nuvem	Características e preço	Apresenta os melhores NGFWs, cita três NGFWs alternativos
[Point 2024b]	Redes de todos os tamanhos	Características	Apresenta a Check Point como o melhor NGFW
Este trabalho	**Data-center**	**Características, opiniões de clientes, vulnerabilidades e *market share***	**Apresenta vulnerabilidades, *market share* e opiniões de usuários**

Tabela 1. Ideia central dos trabalhos relacionados.

Em termos de desafios identificados pelas diferentes análises dos trabalhos, destacam-se: i) a escalabilidade e gestão eficiente das configurações de segurança

em ambientes com recursos limitados [Malmgren and Persson 2016]; ii) custos elevados [Elnerud 2017, eSecurity 2024]; iii) características adicionais ativas reduzem o *throughput* [Elnerud 2017]; iv) a complexidade de gerenciamento (*e.g.*, Fortinet FortiGate) pode exigir maior expertise técnica para configuração e manutenção [Faizan et al. 2019]; v) a proteção de ambientes na nuvem pode ser um desafio para algumas soluções [eSecurity 2024]; e, por fim, vi) escalabilidade [NSSLabs 2014, Malmgren and Persson 2016, Faizan et al. 2019].

3. Metodologia de Investigação

A investigação desenvolvida neste estudo abrange dois pontos principais: uma análise dos principais fabricantes de NGFW e uma análise dos principais produtos desses fabricantes.

Num primeiro estágio do estudo, buscou-se identificar as suas principais características dos NGFWs por meio de uma consulta às documentações (*datasheets*) do respectivo fabricante de cada modelo citado no estudo. Os resultados dessa análise são apresentados na Tabela 2.

Em seguida, num segundo momento do estudo, foram levantados dados comparativos dos fabricantes entre 2023 e 2024. Adicionalmente, foram considerados dados recentemente disponibilizados pelo [6sense 2024], relatório o qual apresenta dados a partir de análises em profundidade de uma variedade de fabricantes de NGFW. Em seguida, foram coletados várias centenas de comentários relatando dificuldades de uso ou implementação de NGFWs no portal Gartner [Gartner 2024]. Para uma compreensão abrangente das vulnerabilidades dos NGFWs analisados no artigo, foram investigadas também as vulnerabilidades conhecidas diretamente nos sites dos respectivos fabricantes, nas áreas específicas de *Security Advisors*, sendo: CheckPoint, Cisco, Fortinet, Huawei, Juniper, Sophos, Palo Alto e Sonicwall. Complementarmente, foram realizadas também pesquisas em duas bases de dados públicas: National Institute of Standards and Technology [Nist 2024], MITRE Corporation [Mitre 2024] e Exploit-DB [Exploit-DB 2024]. As pesquisas foram estruturadas na busca por vulnerabilidades gerais dos firewalls e empresas citadas no artigo. Foram utilizadas as strings de busca `"cve firewall"`, `"Next Generation Firewall"`, `"CVE FIREWALL"`, `"XGS 8500"`, `"Quantum Force 29200"`, `"Firepower 9300 SM-56 x3"`, `"USG 12008"`, `"FortiGate FG 7121F"`, `"CVE SRX 5800 juno os"`, `"PA 7500"`, `"Supermassive 9800"`, `"vulnerabilities firewall"`, `"cisco firewall"`, `"FortiOS"`.

4. Resultados Comparativos de NGFWs e seus Fabricantes

As principais características dos NGFWs estudados são exibidas na Tabela 2, a qual revela uma ampla variedade de capacidades entre os principais produtos de mercado, destacando-se em áreas como segurança e desempenho. Todos os NGFWs listados oferecem recursos avançados, como aprendizado de máquina, prevenção a ataques *zero day*, inspeção profunda de pacotes e detecção de malwares, mostrando um compromisso robusto com a proteção cibernética. No entanto, diferenças notáveis surgem em funcionalidades específicas, como proteção de dispositivos IoT, proteção contra perda de dados e proteção a botnets, onde nem todos os dispositivos oferecem suporte completo.

Característica do NGFW	Quantum Force 29200	Cisco Firepower SM-56 x3	Fortinet Fortigate FG-7121F	Huawei USG 12008	Juniper SRX 5800	Sophos XGS 8500	Palo Alto PA-7500	Sonicwall Supermassive 9800
Aprendizado de máquina	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção a Ataques *Zero Day*	✓	✓	✓	✓	✓	✓	✓	✓
Inspeção profunda de pacotes	✓	✓	✓	✓	✓	✓	✓	✓
Detecção de *Malwares*	✓	✓	✓	✓	✓	✓	✓	✓
Proteção DNS	✓	✓	✓	✓	✓	✓	✓	✗
Proteção a dispositivos IoT	✓	✗	✓	✗	✗	✓	✗	✓
Serviço de IPS/IDS	✓	✓	✓	✓	✓	✓	✓	✓
Filtro URL	✓	✓	✓	✓	✓	✓	✓	✓
Proteção contra perda de Dados	✓	✗	✓	✗	✗	✓	✗	✓
Anti-*Botnet*	✓	✗	✓	✗	✓	✗	✓	✗
Anti-*Spam*	✓	✗	✓	✗	✓	✗	✓	✓
Sandbox Integrada	✓	✓	✓	✗	✓	✗	✓	✓
ProteçãoGPRS, 4G e 5G	✗	✗	✓	✓	✓	✗	✓	✓
Proteção DoS ou DDoS	✓	✓	✓	✓	✓	✓	✓	✓
Configuração Centralizada	✓	✓	✓	✓	✓	✓	✓	✓
Qtd. de dispositivos em série:	**52**	**6**	**16**	**8**	**2**	**16**	**9**	**10**
Deep Packet Inspection (Gbps)	**63,5**	**28**	**540**	**307**	**504**	**34**	**1,5 *Tbps***	**23**
Firewall Throughput (Gbps)	**500**	**235**	**550**	**2,4 *Tbps***	**3,36 *Tbps***	**190**	**1,44 *Tbps***	**31,8**

Tabela 2. Tabela comparativa de funcionalidades entre os NGFWs.

Em 2024, o autor [Inteligence 2024] relatou que a Juniper, Palo Alto, Dell Tecnologies, Huawei e Fortinet podem ser consideradas líderes em tamanho global de mercado. Ao analisar esses dados, percebe-se que o tamanho global de NGFWs pode variar em determinados períodos. Objetivando trazer uma análise mais precisa do tamanho global do mercado de NGFWs, foi realizada uma pesquisa nos dados disponibilizados pela organização 6Sense.com [6sense 2024]. Para oferecer uma visão mais precisa do mercado, utilizamos a quantidade de clientes que utilizam as tecnologias de NGFW como a base de geração do *market share*. Na pesquisa foram relacionadas 61.234 empresas com um total de 99 tecnologias relacionadas. De acordo com a pesquisa [6sense 2024], a Cisco lidera o mercado com 20,3% dos NGFWs comercializados, seguida pela Fortinet com 15,9%, e pela Palo Alto com 11%. As empresas Huawei, Juniper, Check Point, Sophos e Sonicwall, juntas, representam 0,7% do mercado de NGFWs. Esta análise de *market share* pode ser útil para ajudar os consumidores a escolherem seus NGFWs, pois proporciona uma visão clara da popularidade e adoção das diferentes soluções no mercado.

A implementação e operação de NGFWs podem gerar desafios e dificuldades que impactam a satisfação do cliente e a eficácia da solução de segurança. Os problemas comuns enfrentados pelos usuários durante a implementação e uso dos NGFWs foram mapeados através da análise dos comentários desses usuários nos últimos 12 meses no portal Gartner [Gartner 2024], revelando um total de 692 comentários. Destes, 437 (63,15%) foram elogios aos produtos, enquanto 255 (36,85%) expressaram reclamações ou dificuldades na utilização dos NGFWs. A Tabela 3 resume as principais dificuldades relatadas, categorizadas por fabricante.

Por fim, a partir de uma compilação de vulnerabilidades de NGFWs, a qual foi coletada dos sites dos fabricantes e das bases de dados [Nist 2024] [Mitre 2024] e [Exploit-DB 2024], foi elaborada a matriz de vulnerabilidades ilustrada na Figura 1, onde cada item da figura representa uma fonte distinta. Percebe-se que fabricantes Cisco, Palo Alto e Fortinet possuem uma quantidade maior de vulnerabilidades encontradas, o que pode derivar do fato de elas serem líderes no mercado atual e possuírem mais linhas de

	Check Point	Cisco	Fortinet	Huawei	Juniper	Palo Alto	SonicWall	Sophos	Total
Problemas com suporte técnico	29,7%	5,4%	21,6%	5,4%	0%	24,3%	8,1%	5,4%	20,90%
***Bugs* em geral**	7,1%	28,6%	21,4%	7,1%	7,1%	10,7%	14,3	3,6%	15,82%
Dificuldade na Implementação	0%	0%	7,4%	11,1%	7,4%	18,5%	22,2%	33,3%	15,25%
Alto Custo do produto	14,8%	22,2%	11,1%	14,8%	7,4%	29,6%	0%	0%	15,25%
GUI poderia ser melhor	12,0%	40%	4%	8%	4%	4%	16%	12%	14,12%
Visibilidade ruim de Logs	23,1%	7,7%	23,1%	7,7%	0%	7,7%	23,1%	7,7%	7,34%
Problemas de Performance	0%	0%	0%	12,5%	12,5%	37,5%	25%	12,5%	4,52%
Erros no DHCP *Server*	0%	0%	50%	0%	0%	0%	50%	0%	1,13%
Problemas na inspeção Https	50%	50%	0%	0%	0%	0%	0%	0%	1,13%
Problemas no WAF e Proxy	0%	0%	0%	100%	0%	0%	0%	0%	0,56%
Segurança geral do dispositivo	0%	0%	0%	0%	0%	0%	100%	0%	0,56%
Problemas no bloqueio de DNS	100%	0%	0%	0%	0%	0%	0%	0%	0,56%
Alta latência do dispositivo	100%	0%	0%	0%	0%	0%	0%	0%	0,56%
Políticas não centralizadas	100%	0%	0%	0%	0%	0%	0%	0%	0,56%
Dificuldades na recuperação	100%	0%	0%	0%	0%	0%	0%	0%	0,56%
Aplicativos legados no produto	100%	0%	0%	0%	0%	0%	0%	0%	0,56%
Sem 2FA no login	100%	0%	0%	0%	0%	0%	0%	0%	0,56%

Tabela 3. Desafios e dificuldades encontradas de 05/2023 a 05/2024.

produtos em funcionamento. Entretanto, é interessante observar que a Juniper também possui uma alta taxa de vulnerabilidades encontradas, mesmo representando somente menos de 0,7% do mercado de firewalls [6sense 2024].

Na pesquisa por fabricante, a Fortinet se destaca por possuir uma maior quantidade de vulnerabilidades, o que pode ser explicado pelo fato de a empresa possuir vários sistemas operacionais diferentes em seus NGFWs, além de serviços de segurança disponibilizados separadamente que também podem possuir vulnerabilidades. A Sonicwall também se destaca por possuir uma quantidade maior de vulnerabilidades encontradas no site do fabricante, fato esse que pode ser explicado pela sua família de dispositivos possuírem três sistemas operacionais, o SonicOs Gen5, Gen6 e Gen7.

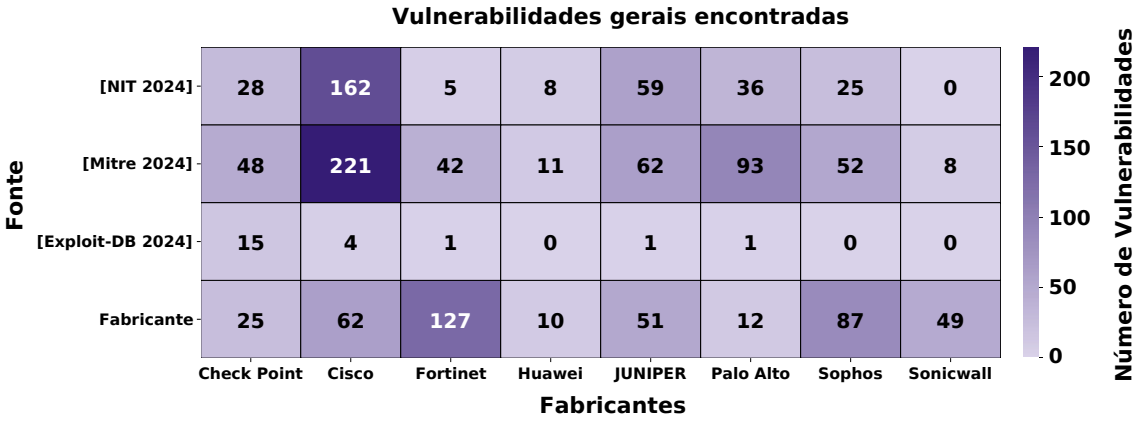

Figura 1. Vulnerabilidades encontradas por fabricante.

5. Conclusão

Este estudo analisou o panorama atual dos NGFWs dos principais fabricantes do mercado. A análise incluiu uma avaliação dos aspectos técnicos, mercadológicos e do *feedback* dos usuários. Também foram destacadas as principais funcionalidades dos NGFWs atuais e os desafios significativos na implementação, custo e suporte técnico. A análise comparativa

de oito ferramentas de NGFWs mostrou variações substanciais em termos de desempenho e funcionalidades. Os dispositivos que mais se destacaram em questão de *throughput* para analisar tráfego criptografado foram o Palo Alto PA-7500, Fortinet Fortigate FG-7121F e Juniper SRX 5800. Já os dispositivos que são mais completos em relação às características avaliadas foram o Check Point Quantum Force 29200 e o Fortinet Fortigate FG-7121F. Além disso, a avaliação das vulnerabilidades conhecidas identificou diferenças significativas entre os fabricantes, o que pode ser parcialmente explicado pelo tamanho de mercado de cada fabricante. Como trabalhos futuros, pretende-se explorar a proteção de dispositivos emergentes, como os de Internet das Coisas (IoT) e redes 5G, que estão cada vez mais presentes em ambientes corporativos e residenciais.

Referências

6sense (2024). Perimeter Security And Firewalls. https://6sense.com/tech/perimeter-security-and-firewalls. Acessado em 01 de Junho 2024.

Alto, P. (2024). PA-7500. https://www.paloaltonetworks.com/resources/datasheets/pa-7500. Acessado em 01 de Junho 2024.

Castro, A. P. (2023). Com pandemia, comércio eletrônico cresce e movimenta 450 bilhões em três anos no país. https://g1.globo.com/economia/noticia/2023/05/11. Acessado em 12 de Maio 2024.

Cisco (2024). Cisco Firepower 9300 Security Appliance. https://www.cisco.com/c/pt_br/support/security/firepower-9300-security-appliance/model.html. Acessado em 29 de Maio 2024.

Elnerud, A. (2017). Comparison of hardware firewalls in a network environment. *Digitala Vetenskapliga Arkivet*, diva2:1106880(35608):29.

eSecurity (2024). Fortinet vs Palo Alto NGFWs: Complete 2024 Comparison. "https://www.esecurityplanet.com/products/fortinet-vs-palo-alto-networks. Acessado em 03 de Junho de 2024.

Exploit-DB (2024). Exploit Database. https://www.exploit-db.com/. Acessado em 03 de Junho de 2024.

Faizan, M., Hcgdc, S., and Yaligar, N. V. (2019). Comparison between Cisco ASA and Fortinet FortiGate. *IOSR J. Comput. Eng.*, 21(3):34–36.

Fortinet (2024). FortiGate 7000F Series. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-7000f-series.pdf. Acessado em 02 de Junho 2024.

Gartner (2024). NETWORK FIREWALLS REVIEWS AND RATINGS. https://www.gartner.com/reviews/market/network-firewalls. Acessado em 25 de Maio 2024.

Huawei (2024). HiSecEngine USG12000 Series AI Firewalls. https://e.huawei.com/en/products/security/usg12000. Acessado em 02 de Junho 2024.

Inteligence, M. (2024). Líderes de mercado de firewall de próxima geração. https://www.delloro.com/news/. Acessado em 13 de Junho de 2024.

Juniper (2024). SRX5400, SRX5600, SRX5800 FIREWALLS DATASHEET. https://www.juniper.net/content/dam/www/assets/datasheets/us/e

n/security/srx5400-srx5600-srx5800-firewall-datasheet.pdf. Acessado em 25 de Maio 2024.

Keary, T. (2024). The Best Next-Gen Firewalls (NGFW) for 2024. https://www.comparitech.com/net-admin/next-gen-firewalls. Acessado em 01 de Junho de 2024.

Liang, J. and Kim, Y. (2022). Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0752–0759. IEEE.

Malmgren, A. and Persson, S. (2016). A comparative study of Palo Alto Networks and Juniper Networks Next-Generation Firewalls for a Small Enterprise Network. *Digitala Vetenskapliga Arkivet*, diva2:934269(31767):45.

Mitre (2024). Search cve list. https://cve.mitre.org/. Acessado em 02 de Junho de 2024.

Neupane, K., Haddad, R., and Chen, L. (2018). Next generation firewall for network security: A survey. In *SoutheastCon 2018*, pages 1–6. IEEE.

Nist (2024). National Vulnerability Database. https://nvd.nist.gov/vuln. Acessado em 02 de Junho de 2024.

Nomios (2024). Top 5 NGFW solutions for 2024. https://www.nomios.com/news-blog/top-5-solutions-ngfw-2024. Acessado em 01 de Junho de 2024.

NSSLabs (2014). Next Generation Firewall Comparative Analysis. https://nsslabs.com. Acessado em 03 de Junho de 2024.

Point, C. (2024a). Quantum Force 29200. https://www.checkpoint.com/downloads/products/quantum-force-29200-datasheet.pdf. Acessado em 25 de Maio de 2024.

Point, C. (2024b). Top 4 Next-Generation Firewalls (NGFWs) Compared. https://www.checkpoint.com/comparison/top-4-ngfw-compared/. Acessado em 17 de Junho de 2024.

Santos, O. T. d. and Nunes, N. P. (2023). Evolução dos crimes cibernéticos na pandemia. Master's thesis, Universidade Federal do Mato Grosso do Sul, Brasil, MS.

Solution, C. a. v. (2023). July 2023 Web Server Survey. https://www.netcraft.com/blog/july-2023-web-server-survey. Acessado em 30 de Maio 2024.

SonicWall (2024). Sonicwall. https://www.sonicwall.com/medialibrary/en/datasheet/datasheet-sonicwall-supermassive-series.pdf. Acessado em 29 de Maio 2024.

Sophos (2024). XGS Series. https://www.sophos.com/en-us/products/next-gen-firewall/tech-specs. Acessado em 01 de Junho 2024.