INTERFACE TECNOLÓGICA

EVOLUÇÃO DOS FIREWALLS E O USO DE NEXT-GENERATION FIREWALL (NGFW)

EVOLUTION OF FIREWALLS AND THE USE OF NEXT-GENERATION FIREWALL (NGFW)

Luigi Enrico Alves Belanda Milani – luigi.milani@fatec.sp.gov.br
Faculdade de Tecnologia de Taquaritinga – Taquaritinga – São Paulo – Brasil

Mauricio de Oliveira Dian - mauricio.dian@fatec.sp.gov.br
Faculdade de Tecnologia de Taquaritinga – Taquaritinga – São Paulo – Brasil

DOI: 10.31510/infa.v22i2.2261
Data de submissão: 01/09/2025
Data do aceite: 01/12/2025
Data da publicação: 20/12/2025

RESUMO

Este artigo analisa a evolução dos *firewalls* e a consolidação dos *firewalls* de próxima geração (*Next-Generation Firewalls* – NGFW) como elementos centrais da segurança da informação. O objetivo foi identificar as limitações dos modelos tradicionais e demonstrar como os NGFW superam essas fragilidades por meio de recursos como inspeção profunda de pacotes, prevenção contra intrusões, visibilidade sobre tráfego criptografado e controle de aplicações. A pesquisa, de caráter bibliográfico e exploratório, evidenciou que os NGFW ampliam a proteção contra ameaças cibernéticas, promovem eficiência operacional e reduzem custos ao unificar múltiplos recursos em uma única plataforma. Verificou-se ainda que sua adoção favorece a implementação de políticas de confiança zero e fortalece a resiliência organizacional. Apesar dos benefícios, destacam-se limitações relacionadas à complexidade de configuração e à necessidade de profissionais qualificados. Conclui-se que os NGFW representam um marco na segurança cibernética contemporânea, respondendo às demandas de ambientes digitais cada vez mais complexos.

Palavras-chave: Firewall. NGFW. Segurança da Informação. Redes de Computadores.

ABSTRACT

This article analyzes the evolution of firewalls and the consolidation of next-generation firewalls (Next-Generation Firewalls – NGFW) as central elements of information security. The objective was to identify the limitations of traditional models and demonstrate how NGFW overcome these weaknesses through features such as deep packet inspection, intrusion prevention, visibility into encrypted traffic and application control. The research, of a bibliographic and exploratory nature, showed that NGFW expand protection against cyber threats, promote operational efficiency and reduce costs by unifying multiple resources on a single platform. It was also found that its adoption favors the implementation of zero trust

policies and strengthens organizational resilience. Despite the benefits, limitations related to configuration complexity and the need for specific professionals stand out. It is concluded that NGFW represent a milestone in contemporary cybersecurity, responding to the demands of increasingly complex digital environments.

Keywords: Firewall. NGFW. Information Security. Computer Networks.

1 INTRODUÇÃO

A segurança da informação tornou-se um pilar estratégico para organizações de todos os portes diante da crescente sofisticação das ameaças cibernéticas. Ataques como ransomwares, phishing, intrusões direcionadas e exploração de vulnerabilidades apresentam velocidade e impacto cada vez maiores, exigindo respostas igualmente avançadas. Segundo a CrowdStrike (2025), o tempo médio para comprometimento de um sistema é de 48 minutos, com registros de apenas 51 segundos, o que evidencia a precisão das ameaças atuais.

Os *firewalls* tradicionais tiveram papel relevante no controle de tráfego e proteção perimetral por meio de filtragem de pacotes e regras predefinidas (Fachinelli; Ahlert, 2019). No entanto, a evolução das técnicas de ataque e a complexidade dos ambientes corporativos revelaram limitações desses modelos, impulsionando o surgimento dos *Next-Generation Firewalls* (NGFWs). Esses dispositivos incorporam recursos como inspeção profunda de pacotes (*Deep Packet Inspection* – DPI), prevenção contra intrusão *(Intrusion Prevention System* – IPS*)*, análise de tráfego criptografado e integração com inteligência artificial, ampliando a capacidade de detecção e mitigação de ameaças (Fortinet, 2025a).

O contexto regulatório reforça essa necessidade. A Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) estabelece diretrizes para o tratamento de dados, tornando a adoção de mecanismos de segurança uma exigência legal. Em âmbito internacional, observa-se movimento semelhante, com regulamentações que demandam conformidade com padrões de proteção (ABES, 2024).

A escolha do tema "Evolução dos *firewalls* e o uso de *Next-Generation Firewall* (NGFW)" fundamenta-se na necessidade de compreender a trajetória da tecnologia, apontar fragilidades dos modelos convencionais e analisar os diferenciais dos NGFWs. Tal abordagem é relevante tanto no campo acadêmico quanto no meio profissional, considerando que incidentes podem ocasionar vazamento de dados, interrupções, prejuízos financeiros e danos à reputação.

Este estudo tem como objetivo analisar a evolução dos *firewalls* até os NGFWs, destacando suas características, benefícios e aplicações em ambientes corporativos. Para isso, será utilizada pesquisa bibliográfica e exploratória baseada em literatura especializada, estudos de caso, relatórios técnicos e documentações de fabricantes reconhecidos no setor a fim de compreender o papel dos NGFWs na segurança cibernética contemporânea e sua contribuição para o fortalecimento das defesas organizacionais.

2 CONCEITO DE FIREWALL E SEGURANÇA DE REDE

A segurança da informação tem como objetivo preservar a confidencialidade, a integridade e a disponibilidade dos dados, garantindo acesso apenas a usuários autorizados, armazenamento adequado e disponibilidade no momento necessário (Fachinelli; Ahlert, 2019). Para Nakamura e Geus (2012), a segurança de redes é essencial à proteção da informação, assegurando tráfego íntegro, confiável e disponível. Além de mitigar ameaças tecnológicas, como ataques de hackers e malwares, também preserva aspectos estratégicos, viabilizando novas oportunidades no ambiente digital. Assim, ao proteger dados, a segurança de redes sustenta a eficiência organizacional e fortalece a confiança de clientes e parceiros.

Nesse contexto, os *firewalls* figuram entre os principais mecanismos de defesa. Conforme a Fortinet (2025b), atuam como barreiras entre redes confiáveis e não confiáveis, inspecionando pacotes de dados e decidindo, conforme regras configuradas, sua permissão ou bloqueio. De acordo com Fachinelli e Ahlert (2019), seus objetivos centrais são: ser imune à penetração, controlar todo o tráfego e constituir o único ponto de entrada e saída da rede. O termo "*firewall*" remete à barreira física à prova de fogo que impede a propagação das chamas entre estruturas (Kurose; Ross, 2010 apud Fachinelli; Ahlert, 2019).

Para este estudo, adota-se a classificação da Fortinet (2025b), que organiza a evolução dos *firewalls* em quatro gerações. A primeira refere-se aos *firewalls* de filtragem de pacotes (*packet filters*), a segunda introduziu os *firewalls* com estado (*stateful*), a terceira, ainda baseada no conceito *stateful*, corresponde aos *firewalls proxy* ou *gateways* de nível de aplicação e a quarta engloba os NGFW.

2.1 Firewalls de 1ª geração

A primeira geração surgiu no final da década de 1980, com a filtragem de pacotes, cujo objetivo era inspecionar dados individuais e aplicar políticas de segurança baseadas em cabeçalhos de pacotes, considerando endereços IP, portas e protocolos de transporte (TCP, UDP etc.) (Fortinet, 2025b). Esse mecanismo operava por listas de regras definidas pelo administrador e podia funcionar de forma *stateless* (estática) ou *stateful* (dinâmica), aplicando os princípios de "permitir tudo que não foi negado" ou "negar tudo que não foi autorizado" (Hoyer; Meirelles; Protector, 2013 apud Fachinelli; Ahlert, 2019).

Segundo a Palo Alto Networks (2024), dispositivos dessa geração atuavam predominantemente em modo *stateless*, tratando pacotes de forma independente, sem armazenar contexto sobre a comunicação. Essa limitação os tornava suscetíveis a ataques como *spoofing* e sequestro de sessão, além de impedir a inspeção da carga útil para detecção de códigos maliciosos.

Apesar dessas fragilidades, os *firewalls* de filtragem de pacotes foram um marco inicial na segurança de redes, estabelecendo as bases para gerações posteriores. Seu baixo custo e simplicidade favoreceram ampla adoção, embora suas limitações tenham impulsionado o desenvolvimento da segunda geração, capaz de realizar inspeção com estado (*stateful inspection*) e oferecer maior segurança (Palo Alto Networks, 2024; Fortinet, 2025b).

2.2 Firewalls de 2ª geração

Os *firewalls* de segunda geração, ou *stateful firewalls*, surgiram no início dos anos 2000, aprimorando a filtragem de pacotes por meio do monitoramento do estado das conexões (FORTINET, 2025b). Diferentemente dos filtros tradicionais, que analisavam apenas cabeçalhos de pacotes sem considerar o histórico da comunicação (Stallings, 2017), os *stateful firewalls* registram sessões em uma tabela de estados com informações como endereços IP, portas e status da conexão, bloqueando pacotes que se desviam do fluxo esperado (Scarfone; Hoffman, 2009).

Sua principal vantagem reside na análise contextual do tráfego, oferecendo maior segurança em relação à filtragem estática (Nakamura; Geus, 2012), sem comprometer o desempenho, já que pacotes subsequentes podem ser verificados diretamente na tabela de estados (Fachinelli; Ahlert, 2019).

Apesar do avanço, esses dispositivos atuam predominantemente nas camadas de rede e transporte (2 a 4 do modelo OSI), apresentando limitações na inspeção em nível de aplicação, o que dificulta a diferenciação de tráfego e a detecção de vazamento de informações (Fachinelli; Ahlert, 2019).

Assim, os *stateful firewalls* representaram um marco na segurança de redes, mas a crescente sofisticação das ameaças e a complexidade dos sistemas evidenciaram suas limitações (Maneca, 2015).

2.3 Firewalls de 3ª geração

A terceira geração de *firewalls* surgiu para superar as limitações das anteriores. Enquanto a primeira restringia-se aos cabeçalhos de pacotes e a segunda adicionava a inspeção de estado, os *firewalls proxy* ou *gateways* de aplicação passaram a atuar diretamente na camada de aplicação. Segundo Stallings (2017), esses dispositivos funcionam como retransmissores do tráfego, mediando a comunicação entre cliente e servidor. Nesse modelo, cada tentativa de conexão gera duas sessões distintas — cliente-*proxy* e *proxy*-destino — ocultando os endereços internos da rede (Scarfone; Hoffman, 2009).

Além da análise de cabeçalhos, os proxies inspecionam comandos e conteúdos específicos, permitindo, por exemplo, bloquear anexos em e-mails, restringir comandos críticos em FTP, aplicar políticas de navegação ou rejeitar certificados digitais de autoridades não confiáveis. Sua aplicabilidade abrange protocolos como HTTP, SMTP, POP, IMAP e VoIP (Scarfone; Hoffman, 2009).

Entretanto, apresentam desvantagens significativas. A necessidade de examinar e retransmitir todo o tráfego gera sobrecarga de processamento, tornando-os inadequados para aplicações de alta largura de banda ou tempo real (Stallings, 2017; Scarfone; Hoffman, 2009). Além disso, demandam agentes *proxy* específicos para cada protocolo, limitando escalabilidade e flexibilidade.

Em síntese, os *firewalls proxy* marcaram a evolução da segurança perimetral ao introduzir a inspeção em nível de aplicação. Apesar de suas limitações, estabeleceram a base conceitual para os NGFW, que integram análise profunda de pacotes, prevenção de intrusões e controle de aplicações (Fachinelli; Ahlert, 2019).

2.4 Firewalls de 4ª geração

Os *firewalls* de próxima geração, NGFW, representam a evolução da segurança de redes ao integrarem, em uma única solução, funções avançadas de inspeção e controle de tráfego. Diferentemente dos modelos tradicionais, permitem análise contextual de aplicações, detecção de intrusões, visibilidade sobre tráfego criptografado e integração com inteligência contra ameaças (Morais et al., 2024). Em estudo comparativo, Morais et al. (2024) destacam fornecedores como Check Point, Cisco, Fortinet, Huawei, Juniper, Palo Alto, SonicWall e Sophos, ressaltando a incorporação de Inteligência Artificial (IA) e Aprendizado de Máquina (AM) em seus recursos.

Embora compartilhem funções com os *stateful firewalls,* como VPNs e controle de portas e protocolos, Maneca (2015) destaca que a principal diferença está na consolidação de múltiplos recursos em uma única plataforma. Em um único equipamento físico ou virtual, os NGFW podem oferecer IDS/IPS, controle de aplicações, filtragem web, antivírus, monitoramento de estações e QoS, configurando-se como ferramentas centrais de proteção corporativa. Ainda segundo Maneca (2015), essa evolução representa um marco na forma de estruturar a segurança de rede, ao passo que fabricantes como a Fortinet (2025b) ressaltam que os NGFW combinam as melhores características das gerações anteriores com capacidades avançadas para mitigar ataques modernos, simplificando e centralizando a proteção em ambientes distribuídos. O modelo Fortigate 70F, por exemplo, utiliza mais de 18.000 assinaturas em seu sistema de prevenção de intrusões (IPS), aliado a recursos de IA/AM para inspeção profunda de pacotes e SSL, possibilitando detectar conteúdos maliciosos e aplicar *patches virtuais* em vulnerabilidades recém-descobertas (Fortinet, 2025a). Entre seus diferenciais, a fabricante aponta a prevenção contra ameaças *zero-day* com detecção em tempo real, a integração com a matriz MITRE ATT&CK e a redução da sobrecarga operacional. Além disso, outros recursos incluem prevenção de perda de dados (*Data Loss Prevention* - DLP), segurança para dispositivos IoT, *sandboxing* em rede e integração com SD-WAN (Fortinet, 2025b).

O Gartner (2020) define os NGFW como *firewalls* de inspeção profunda que vão além da análise por portas e protocolos, incorporando inspeção em nível de aplicação, prevenção de intrusões e inteligência externa, ressaltando que não devem ser confundidos com a simples junção de *firewall* e IPS. Heino, Hakkala e Virtanen (2022) complementam que, diferentemente dos *firewalls* de primeira geração, restritos ao bloqueio de endereços IP e portas, os NGFWs surgiram para superar a ausência de visibilidade da camada de aplicação. Esses dispositivos,

cujo conceito foi introduzido pela Palo Alto Networks em 2010, incorporam inspeção profunda de pacotes, permitindo maior controle do tráfego com base em protocolos de aplicação e políticas associadas a identidades de usuários e grupos. Além disso, oferecem suporte a recursos como VPNs IPsec/SSL, *routing* e NAT, além de serem escaláveis em versões físicas, virtuais e como serviço em nuvem (*Firewall as a Service* – FWaaS).

A evolução contínua dos NGFW acompanha mudanças no cenário de ameaças e nos modelos de trabalho. O avanço da mobilidade corporativa e a adoção de ambientes híbridos impulsionaram o desenvolvimento de arquiteturas mais complexas, como o *Secure Access Service Edge* (SASE), introduzido pelo Gartner em 2019, que combina FWaaS e SD-WAN para atender à demanda crescente por soluções de segurança distribuídas e otimizadas para o trabalho remoto (Heino; Hakkala; Virtanen, 2022). Nesse contexto, os NGFW consolidam-se como elementos estratégicos para a proteção de redes modernas, capazes de responder a ameaças sofisticadas com maior eficiência e abrangência.

3 PROCEDIMENTOS METODOLÓGICOS

Este estudo caracteriza-se como uma pesquisa de natureza exploratória e bibliográfica, fundamentada em referências acadêmicas, relatórios técnicos e documentações de fabricantes especializados. A abordagem adotada busca compreender a evolução histórica dos *firewalls* e analisar as funcionalidades e aplicações dos NGFWs.

A coleta de dados foi realizada por meio da consulta a livros, artigos científicos, teses, dissertações, relatórios de mercado e publicações de empresas do setor de cibersegurança. Essa estratégia permitiu identificar tendências, limitações dos modelos tradicionais e avanços trazidos pelos NGFWs. A metodologia adotada possibilitou uma análise comparativa entre as diferentes gerações de *firewalls*, relacionando suas características técnicas e o impacto de sua adoção em ambientes corporativos.

4 RESULTADOS E DISCUSSÃO

Os NGFW representam um marco na evolução da segurança da informação, ao integrarem funcionalidades avançadas que transcendem as limitações dos *firewalls* tradicionais. Enquanto os modelos anteriores atuavam principalmente com base em portas e protocolos, os NGFW incorporam inspeção profunda de pacotes, controle de aplicações, prevenção de

intrusões e visibilidade granular sobre usuários e dispositivos, proporcionando um nível mais abrangente de proteção (Maneca, 2015). Além disso, estudos recentes destacam que tais dispositivos evoluíram para atender à crescente sofisticação das ameaças digitais, consolidando-se como soluções essenciais no cenário atual (Morais et al., 2024).

A crescente complexidade dos ambientes digitais contemporâneos exige soluções de segurança capazes de lidar com ameaças cada vez mais sofisticadas. O Relatório Global de Ameaças 2025 da CrowdStrike como apontado também no começo deste artigo destaca que o tempo médio para comprometimento em ataques caiu para apenas 48 minutos em 2024, com registros de invasões em menos de um minuto, evidenciando a velocidade com que os adversários se adaptam às defesas e exploram novas tecnologias, como a inteligência artificial generativa, para potencializar campanhas de engenharia social e desinformação (Crowdstrike, 2025). De modo semelhante, o relatório global da Fortinet ressalta que mais de 40% dos ataques de ransomware em 2023 foram direcionados ao setor industrial e de tecnologia operacional (*Operational Technology* - OT), comprometendo cadeias de suprimentos críticas e explorando vulnerabilidades em dispositivos IoT e sistemas legados (Fortiguard Labs, 2023a).

Esse cenário é agravado pela escassez de profissionais de cibersegurança e pela ampliação da superfície de ataque digital em razão da convergência entre TI e OT, conforme observado no Relatório de Cibersegurança OT 2024, que aponta que quase um terço das organizações sofreu seis ou mais intrusões apenas no último ano, com impactos diretos em produtividade, receita e até mesmo riscos à segurança física (Fortinet, 2024). O panorama se torna ainda mais crítico quando se consideram os ataques à cadeia de suprimentos, cujo crescimento foi de 650% em 2021 e que seguem como vetor de ameaça relevante, explorando vulnerabilidades amplamente distribuídas em serviços de nuvem e softwares utilizados globalmente (Check Point, 2022).

Justamente um dos principais benefícios associados ao uso de NGFW é a melhoria significativa na postura de segurança das organizações. Segundo a Forrester (2022), soluções como o Cisco Secure Firewall reduziram o risco de violação material em até 80%, além de possibilitarem a mitigação rápida de incidentes por meio de plataformas integradas de análise e resposta, como o SecureX. Ainda de acordo com a consultoria, o Fortinet NGFW demonstrou eficiência em ambientes de *data center*, alcançando redução de 50% em falhas de rede e ganhos de produtividade de equipes de segurança e usuários finais, com retorno sobre investimento (ROI) de 318% em três anos (Forrester, 2023).

Além da proteção contra ameaças, os NGFW contribuem para ganhos de eficiência operacional e redução de custos. A Forrester (2022) também relata que a unificação de múltiplos recursos de segurança em uma única plataforma permite substituir soluções legadas, simplificando o gerenciamento e reduzindo a complexidade administrativa. Na mesma pesquisa, foram indicadas reduções de até 95% no tempo necessário para atualizações de políticas de *firewall* e de 83% no esforço de investigação de incidentes, liberando recursos humanos para atividades estratégicas.

Outro aspecto relevante é a visibilidade ampliada sobre usuários, aplicações e dispositivos conectados. Essa característica, viabilizada por técnicas de inspeção em tráfego criptografado e heurísticas comportamentais, possibilita a aplicação de políticas contextuais e dinâmicas, alinhadas ao paradigma de confiança zero (*zero trust*) (Fortinet, 2023b). Essa capacidade favorece tanto a proteção de dados sensíveis quanto a continuidade dos negócios em ambientes híbridos e distribuídos, onde grande parte do tráfego é criptografado (Moraes; Silva, 2024).

Do ponto de vista econômico, os benefícios são igualmente expressivos. Estudos independentes mostram que a substituição de múltiplas soluções por NGFW reduziu custos com licenciamento em até 40%, além de otimizar o consumo energético em data centers graças ao uso de processadores de segurança dedicados (Forrester, 2023). Esses resultados evidenciam que os NGFW não apenas reforçam a segurança, mas também contribuem para a sustentabilidade e a racionalização de recursos organizacionais.

Em síntese, os NGFW oferecem vantagens que combinam segurança avançada, eficiência operacional e retorno financeiro. Sua adoção possibilita às organizações mitigar riscos cibernéticos, otimizar processos internos e atender a requisitos regulatórios, configurando-se como solução estratégica diante da crescente complexidade dos ambientes digitais contemporâneos.

5 CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo analisar a evolução dos *firewalls* até a consolidação dos NGFW como ferramentas estratégicas na segurança da informação. Esse objetivo foi alcançado a partir de uma revisão bibliográfica e documental, que permitiu compreender as limitações das gerações anteriores e demonstrar como os NGFW superam tais fragilidades ao integrar funcionalidades avançadas, como inspeção profunda de pacotes,

prevenção contra intrusões, visibilidade ampliada de tráfego criptografado e controle contextual de aplicações.

Os resultados indicam que os NGFW representam não apenas uma evolução tecnológica, mas também uma resposta estratégica às exigências de ambientes digitais contemporâneos, caracterizados pela sofisticação crescente das ameaças, pela convergência entre TI e OT e pela adoção de infraestruturas híbridas e em nuvem. Além de ampliarem a proteção contra ataques, essas soluções contribuem para eficiência operacional, redução de custos e aderência a modelos de governança baseados no paradigma de confiança zero, fortalecendo a resiliência organizacional.

Moraes e Silva (2024) apontam que, embora os NGFW ofereçam ampla proteção, sua implementação pode se tornar um desafio devido à complexidade de configuração em ambientes híbridos ou em nuvem, o que exige treinamento ou até a contratação de especialistas em segurança cibernética. Ainda segundo os autores, esse cenário reforça que o simples investimento em tecnologia não é suficiente sem o devido preparo técnico. Na mesma linha, Morais et al. (2024) destacam que, ao integrarem múltiplos recursos avançados, as soluções de NGFW podem aumentar a dificuldade de uso e implementação. Isso implica, segundo eles, em uma demanda por maior especialização técnica das equipes de TI. Complementando esse raciocínio, a Forrester (2023) observa que organizações que já adotaram NGFWs relataram dificuldades especialmente ligadas à manutenção e atualização desses sistemas em infraestruturas híbridas. Tal constatação reforça a necessidade de profissionais capacitados para garantir a eficácia da proteção oferecida.

Como perspectiva futura, sugere-se o aprofundamento de estudos empíricos que avaliem o desempenho de NGFW em diferentes setores econômicos e contextos de infraestrutura, considerando métricas de tempo de resposta, impacto financeiro e escalabilidade. Além disso, pesquisas voltadas à integração dos NGFW com arquiteturas emergentes, como *zero trust* e SASE, podem ampliar a compreensão de sua aplicabilidade em cenários de trabalho remoto, IoT e ambientes altamente distribuídos.

Em síntese, conclui-se que os NGFW se consolidam como instrumentos indispensáveis para a segurança da informação, atendendo às necessidades atuais das organizações e apontando caminhos promissores para a proteção de dados em um cenário digital cada vez mais complexo. Apesar das dificuldades apontadas, os benefícios decorrentes de sua utilização superam os desafios, tornando o uso dos NGFW altamente vantajoso para empresas e demais instituições que buscam fortalecer suas estratégias de segurança.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE - ABES. **Como o firewall de próxima geração garante a proteção dos dados e a conformidade com regulamentações - ABES**. ABES, 2024. Disponível em: <https://abes.com.br/como-o-firewall-de-proxima-geracao-garante-a-protecao-dos-dados-e-a-conformidade-com-regulamentacoes/>. Acesso em: 05 jun. 2025.

CHECK POINT. **Relatório de Segurança Cibernética 2022**. Check Point, 2022. Disponível em: <https://www.checkpoint.com/downloads/resources/cyber-security-report-2022.pdf> Acesso em: 10 ago. 2025.

CROWDSTRIKE. **Relatório global de ameaças 2025**. Crowdstrike, 2025. Disponível em: <https://www.crowdstrike.com/en-us/global-threat-report/>. Acesso em: 02 abr. 2025.

FACHINELLI, M.; AHLERT, E. M. **Firewall de próxima geração - Fortinet**. Revista Destaques Acadêmicos, [S. l.], v. 11, n. 4, 2019. DOI: 10.22410/issn.2176-3070.v11i4a2019.2385. Disponível em: <https://univates.br/revistas/index.php/destaques/article/view/2385>. Acesso em: 02 abr. 2025.

FORRESTER. **The Total Economic Impact of Cisco Secure Firewall.** Forrester Consulting, 2022. Disponível em: <https://www.cisco.com/c/dam/global/en_ca/products/collateral/security/forrester-secure-firewall-tei-study.pdf>. Acesso em: 17 ago. 2025.

FORRESTER. **The Total Economic Impact of Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution.** Forrester Consulting, 2023.

FORTIGUARD LABS. **Relatório de Cenário de Ameaças Global – 2º semestre de 2023**. Fortinet, 2023a. Disponível em: <https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/pt_br/report-2023-threat-landscape.pdf>. Acesso em: 09 ago. 2025.

FORTINET. **Enable Deep Visibility for Applications, Users and Devices with FortiGate NGFW.** Fortinet, 2023b. Disponível em: <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortigate-visibility.pdf>. Acesso em: 20 jul. 2025.

FORTINET. **Relatório 2024 sobre o Estado da Tecnologia Operacional e Cibersegurança**. Fortinet, 2024. Disponível em: <https://www.fortinet.com/content/dam/fortinet/assets/reports/pt_br/report-state-ot-cybersecurity.pdf>. Acesso em: 20 jul. 2025.

FORTINET. **FortiGate 70F Series Data Sheet**. Fortinet, 2025a. Disponível em: <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-70f-series.pdf>. Acesso em: 05 abr. 2025.

FORTINET. **O que é firewall de rede?**. Fortinet, 2025b. Disponível em:

<https://www.fortinet.com/br/resources/cyberglossary/firewall>. Acesso em: 05 abr. 2025.

HEINO, J.; HAKKALA, A.; VIRTANEN, S. **Study of methods for endpoint aware inspection in a next generation firewall.** Cybersecurity, v. 5, n. 1, p. 25, 2022. DOI: 10.1186/s42400-022-00127-8. Disponível em: <https://pmc.ncbi.nlm.nih.gov/articles/PMC9439937/>. Acesso em: 16 ago. 2025.

GARTNER. **Next-Generation Firewalls (NGFWs**). Gartner, 2020. Disponível em: <https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws>. Acesso em: 16 ago. 2018.

MANECA, M. A. M. B. **Firewalls, a próxima geração**. Tese (Mestrado em Segurança Informática) - Faculdade de Ciências - Departamento de Informática, Universidade de Lisboa. Lisboa, p. 72. 2015. Disponível em: <https://repositorio.ulisboa.pt/handle/10451/23557>. Acesso em: 31 maio 2025.

MORAIS, T. W. et al. **Firewalls de Próxima Geração (NGFW): Funcionalidades, Aplicações e Vulnerabilidades.** In: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 24., 2024, São José dos Campos/SP. Anais... Porto Alegre: Sociedade Brasileira de Computação, 2024. p. 801-807. DOI: 10.5753/sbseg.2024.241781. Disponível em: <https://sol.sbc.org.br/index.php/sbseg/article/view/30071>. Acesso em 27 jul. 2025.

MORAES, W. S.; SILVA, S. **Estudo do firewall Fortigate da Fortinet para auxiliar na segurança de dados de uma empresa.** III Jornada Científica da Escola Politécnica e de Artes, Goiânia, 2024. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7991>. Acesso em: 16 ago. 2025.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos**. 1 ed. São Paulo: Novatec, 2012. 483 p.

PALO ALTO NETWORKS. **History of Firewalls**. [S. l.]: Palo Alto Networks, 2024. Disponível em: <https://www.paloaltonetworks.com/cyberpedia/history-of-firewalls>. Acesso em: 02 ago. 2025.

SCARFONE, K.; HOFFMAN, P. **Guidelines on Firewalls and Firewall Policy**. Gaithersburg: National Institute of Standards and Technology (NIST), 2009. (Special Publication 800-41, Rev. 1). Disponível em: <https://www.nist.gov/publications/guidelines-firewalls-and-firewall-policy>. Acesso em: 08 ago. 2025.

STALLINGS, W. **Network Security Essentials: Applications and Standards**. 6. ed. Boston: Pearson, 2017.