Especificação de Requisitos de Segurança em Firewalls de Próxima Geração: Abordagens e Desafios

Tiago W. Morais[1], Felipe H. Scherer[1], Felipe N. Dresch[1], Silvio E. Quincozes[1], Diego Kreutz[1], Vagner E. Quincozes[2]

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

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

{tiagomorais, felipescherer, felipedresch}.aluno@unipampa.edu.br

{silvioquincozes, diegokreutz}@unipampa.edu.br

vequincozes@midiacom.uff.br

Abstract. *This work specifies the framework MORAIS, which offers initial directions to assist development teams in structuring and validating security requirements in developing Next Generation Firewalls (NGFWs), considering adaptation to dynamic threats and compliance with regulations. The steps of the framework include* ***M****onitoring,* ***O****ptimization,* ***A****uditing,* ***R****equirements,* ***I****ntegration and* ***S****imulation, allowing a structured approach to address the main performance, integration and compliance challenges. The results obtained through a proof of concepts indicate that implementing MORAIS can bring continuous improvement, adaptability, and effectiveness to NGFWs.*

Resumo. *Este trabalho especifica o framework MORAIS, o qual oferece direções iniciais para auxiliar equipes de desenvolvimento na estruturação e validação de requisitos de segurança no desenvolvimento de Firewalls de Próxima Geração (NGFWs), considerando a adaptação às ameaças dinâmicas e a conformidade com regulamentações. As etapas do framework incluem* ***M****onitoramento,* ***O****timização,* ***A****uditoria,* ***R****equisitos,* ***I****ntegração e* ***S****imulação, permitindo uma abordagem estruturada para enfrentar os principais desafios de desempenho, integração e conformidade. Os resultados obtidos através de uma prova de conceitos indicam que a implementação do MORAIS pode trazer melhorias contínuas, adaptabilidade e eficácia para NGFWs.*

1. Introdução

A crescente sofisticação das ameaças cibernéticas tem pressionado as organizações a adotarem soluções de segurança mais avançadas, como so *firewalls* de Próxima Geração, do inglês *Next-Generation Firewalls* (NGFWs). Os NGFWs oferecem funcionalidades que vão além da simples filtragem de pacotes, integrando inspeção profunda de tráfego, controle de aplicativos e detecção de ameaças avançadas [Rajkumar and Arunakranthi 2023]. No entanto, o sucesso desses sistemas de proteção depende diretamente de uma boa definição de requisitos durante seu desenvolvimento. No contexto de NGFWs, onde é crucial que os sistemas operem de maneira eficaz contra ameaças cibernéticas emergentes, a correta definição de requisitos desde o início pode reduzir drasticamente a probabilidade de falhas operacionais e de segurança. A documentação precisa e a gestão contínua

de mudanças nos requisitos são elementos chave para o sucesso e evolução destes sistemas [PMI 2010].

Estudos apontam que cerca de 71% dos projetos de software falham devido a uma gestão inadequada de requisitos, o que pode incluir a falta de clareza, especificações incompletas e mudanças contínuas durante o ciclo de vida do projeto [Hussain and Mkpojiogu 2016]. Esses problemas podem resultar em um aumento nos custos de desenvolvimento, atrasos significativos e até a inviabilidade do produto final. A engenharia de requisitos aliada a experiências anteriores podem ser usadas para extrair recursos importantes que ajudarão a resolver esses problemas com mais eficiência [Shaheed and Kurdy 2022]. Isso reforça a justificativa para a aplicação de um processo estruturado de engenharia de requisitos.

Este trabalho tem como objetivo principal propor um *framework* para a especificação de requisitos de segurança em NGFWs, visando enfrentar os desafios relacionados à adaptação às ameaças cibernéticas dinâmicas e à conformidade com regulamentações. A proposta deste *framework*, denominado **MORAIS**, busca fornecer diretrizes que orientem o desenvolvimento de NGFWs com foco em segurança contínua, otimização de desempenho, auditoria e integração com outros sistemas de segurança. O nome **MORAIS** é um acrônimo para as etapas do *framework*: **M**onitoramento, **O**timização, **R**equisitos, **A**uditoria, **I**ntegração e **S**imulação, cobrindo os aspectos críticos do desenvolvimento e operação de NGFWs.

As principais contribuições deste trabalho incluem a definição de um conjunto de etapas estruturadas que auxiliam no processo de elicitação e validação de requisitos de segurança, além da implementação de mecanismos que permitam o monitoramento contínuo e a adaptação do NGFW a novos cenários de ataque. A estrutura deste trabalho está organizada da seguinte forma: inicialmente, é apresentada uma revisão das metodologias existentes para especificação de requisitos de segurança em NGFWs; em seguida, o *framework* **MORAIS** é introduzido e detalhado, abordando suas principais funcionalidades. Por fim, um estudo de caso é apresentado para demonstrar a aplicação prática do *framework*, seguido das considerações finais.

2. Metodologias de Especificação de Requisitos de Segurança

A especificação de requisitos de segurança em NGFWs é um processo crítico, uma vez que esses dispositivos devem ser projetados para mitigar uma vasta gama de ameaças cibernéticas, conhecidas ou não, atendendo a demandas específicas de segurança em ambientes cada vez mais complexos. O processo de elicitação e modelagem desses requisitos de segurança pode ser desafiador, especialmente devido à natureza dinâmica das ameaças e à crescente complexidade dos sistemas de tecnologia da informação. Para lidar com essas questões, metodologias estruturadas de especificação de requisitos são essenciais.

Uma das abordagens mais comumente usadas para a especificação de requisitos de segurança em sistemas críticos, como os NGFWs, é o *Threat Modeling*, metodologia que foca na identificação de ameaças e vulnerabilidades potenciais, permitindo que engenheiros de software e segurança desenvolvam mecanismos de proteção adequados. No contexto dos NGFWs, o *Threat Modeling* ajuda a mapear possíveis vetores de ataque, como a exploração de vulnerabilidades de rede, ataques a aplicativos e interceptação de pacotes de dados [Xiong and Lagerström 2019]. O modelo *STRIDE*, amplamente utilizado no

Threat Modeling, categoriza as ameaças em seis grupos: *Spoofing* (falsificação), *Tampering* (manipulação), *Repudiation* (não repúdio), *Information Disclosure* (divulgação de informações), *Denial of Service* (negação de serviço) e *Elevation of Privilege* (elevação de privilégio) [Hussain et al. 2014]. No contexto de NGFW, essas ameaças podem se manifestar de diferentes formas, como ataques de falsificação de identidade para obter acesso a redes protegidas, ou ataques de negação de serviço visando comprometer a disponibilidade dos serviços de *firewall* [Makhdoomi et al. 2022].

Outra metodologia relevante para a especificação de requisitos de segurança em NGFWs é o uso de modelos voltados à proteção de privacidade, como o *LINDDUN*. Esse modelo é utilizado para identificar ameaças de privacidade ao longo do ciclo de vida do sistema e é particularmente útil quando o NGFW também lida com dados pessoais ou sensíveis [Nweke, Livinus Obiora et al. 2022]. O *LINDDUN* categoriza as ameaças em sete classes: *Linkability* (vinculação), *Identifiability* (identificabilidade), *Non-repudiation* (não repúdio), *Detectability* (detectabilidade), *Disclosure of Information* (divulgação de informações), *Unawareness* (falta de conscientização) e *Non-compliance* (não conformidade). No contexto de NGFW, esse modelo pode ser aplicado para garantir que o *firewall* não apenas previna ataques, mas também mantenha a conformidade com regulamentações de privacidade, como o Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* – GDPR), e preserve os dados pessoais processados pela rede [Nweke, Livinus Obiora et al. 2022].

Para facilitar a compreensão das metodologias de especificação de requisitos de segurança, é comum utilizar cenários práticos e casos de uso. Um exemplo de aplicação de *Threat Modeling* no desenvolvimento de um NGFW pode envolver a definição de um caso de uso onde o *firewall* precisa identificar e bloquear ataques de negação de serviço distribuídos (*Distributed Denial of Service* – DDoS). O *Threat Modeling* pode ser usado para antecipar os métodos de ataque e, a partir disso, especificar requisitos de mitigação, como a capacidade do NGFW de monitorar grandes volumes de tráfego e identificar padrões anômalos.

Por fim, *Frameworks* como o *Security Quality Requirements Engineering* (*SQUARE*) fornecem uma abordagem sistemática para a elicitação, análise e priorização de requisitos de segurança. O *SQUARE* envolve nove etapas, incluindo a identificação de metas de segurança, a categorização de requisitos e a análise de possíveis *trade-offs*. No caso dos NGFWs, o uso de *SQUARE* pode ajudar a garantir que os requisitos de segurança sejam bem definidos desde o início, levando em consideração as ameaças emergentes e os requisitos de desempenho.

3. Trabalhos Relacionados

Existem estudos que abordam requisitos de segurança em sistemas. Por exemplo, os autores [Morić et al. 2024] avaliam a viabilidade e as implicações práticas da implementação de um *framework Zero Trust Architecture* (ZTA) em uma grande empresa de saúde, comparando com o modelo tradicional de segurança baseado em perímetro (PBSM). Outro trabalho [Mishra, A. et al. 2024] propõe uma análise de metadados sobre a especificação de requisitos de segurança usando métodos formais. A proposta inclui a utilização de métodos formais como Z, Lotos e outras linguagens matemáticas para especificar requisitos de segurança de forma que possam ser verificados automaticamente, garantindo que

os sistemas estejam alinhados com os requisitos desde a fase inicial de desenvolvimento.

Além disso, há *frameworks* que buscam padronizar a medição e especificação de requisitos de segurança em fases iniciais de desenvolvimento de software. Um exemplo é o uso de normas internacionais como ECSS, IEEE e ISO, combinado com a ISO 19761 (COSMIC), para medir funcionalidades de segurança, auxiliando engenheiros a garantir disponibilidade, confidencialidade e integridade durante a fase de requisitos não funcionais [Meridji et al. 2019]. Também há métodos que realizam a elicitação de requisitos de segurança a partir de modelos de processos de negócios [Ahmed and Matulevicius 2014], possibilitando a captura das necessidades de segurança da empresa e traduzindo-as em requisitos de segurança para o sistema a ser desenvolvido.

Diferente dessas propostas, que têm um foco mais amplo em sistemas ou abordagens genéricas de segurança, o *framework* MORAIS destaca-se por focar especificamente em NGFWs. Ele oferece uma solução completa, incluindo monitoramento contínuo, otimização de desempenho e conformidade com regulamentações, alinhando a segurança com as demandas específicas de desempenho e adaptabilidade desses sistemas críticos.

O trabalho [Singh and Cheema 2023] aborda a temática dos NGFWs de maneira mais específica, detalhando as vantagens da nova geração em comparação com os tipos tradicionais de *firewalls*. Ainda, os autores listam uma série de requisitos de segurança considerados de alta importância e analisam as soluções de *hardware* e *software* oferecidas pelas empresas mais conhecidos no ramo. Ademais, um *framework* de autoautenticação para ambientes distribuídos é proposto no estudo, funcionalidade que destaca a necessidade de monitoramento contínuo da rede para garantir a integridade do sistema e está, portanto, alinhada com a primeira etapa do *framework* MORAIS.

4. Desafios na Definição e Validação dos Requisitos

Devido à natureza dinâmica das ameaças cibernéticas e à crescente complexidade das redes, o desenvolvimento de NGFWs enfrenta uma série de desafios na definição e validação de requisitos de segurança. Estes desafios exigem que a engenharia de requisitos vá além da simples especificação de funcionalidades, concentrando-se também na definição de mecanismos que permitam a adaptação contínua do *firewall* a novos cenários de ataque e à evolução das regulamentações de proteção de dados.

Um dos principais desafios na definição de requisitos é o equilíbrio entre oferecer uma proteção robusta e manter o desempenho da rede. Funcionalidades como inspeção profunda de pacotes (DPI), prevenção de intrusões e controle de aplicativos são cruciais para a segurança, mas podem impactar significativamente a latência e a largura de banda da rede [Hamilton, Robert et al. 2020]. A sobrecarga introduzida pelo processamento detalhado de pacotes, combinado com a necessidade de análise em tempo real, pode criar gargalos e prejudicar a experiência do usuário. Para mitigar esses efeitos, é essencial que os requisitos de desempenho sejam claramente definidos durante a fase de engenharia de requisitos. Estes podem incluir a definição de limites de latência aceitáveis, requisitos de escalabilidade para lidar com altos volumes de tráfego e diretrizes para a implementação eficiente de algoritmos de detecção. Testes de desempenho também devem ser realizados regularmente para garantir que as melhorias de segurança não prejudiquem o fluxo normal de dados na rede.

A conformidade com regulamentações adiciona outra camada de complexidade

ao desenvolvimento de *firewalls*. Os requisitos relacionados à privacidade e à proteção de dados não podem ser ignorados, e qualquer falha em aderir a essas regulamentações pode resultar em multas substanciais e danos à reputação da organização e dos usuários. Os *firewalls* devem ser projetados para permitir auditorias, fornecer registros detalhados e garantir a privacidade dos dados trafegados [Drkag and Szymura 2018]. Um *firewall* que esteja em conformidade hoje pode se tornar obsoleto amanhã com a introdução de novas normas ou a reformulação de regulamentações existentes. Assim, a engenharia de requisitos deve antecipar essas mudanças e incluir diretrizes para atualizações periódicas e monitoramento contínuo das regulamentações relevantes.

A integração de *firewalls* com outras soluções de segurança, como Sistemas de Gestão de Eventos de Segurança (SIEM) e Sistemas de Detecção de Intrusões (IDS), é outro desafio significativo. A interoperabilidade entre essas plataformas é crucial para permitir a correlação de eventos e uma visão holística da segurança da rede. Sem essa integração, a análise de ameaças pode se tornar fragmentada, prejudicando a resposta eficaz a incidentes [Abusamrah et al. 2021]. Os requisitos de integração devem ser bem especificados, incluindo a compatibilidade com APIs, formatos de dados e protocolos de comunicação. É importante garantir que o *firewall* possa se comunicar de forma eficaz com sistemas externos e que a transferência de dados entre essas plataformas seja segura e eficiente. Ademais, a validação desses requisitos deve incluir testes rigorosos para verificar a interoperabilidade entre o *firewall* e os sistemas existentes.

Finalmente, é importante reforçar que as ameaças cibernéticas estão em constante evolução, e os *firewalls* devem ser projetados para se adaptar rapidamente a novos tipos de ataques. Esse desafio é agravado pela necessidade de os *firewalls* reconhecerem e bloquearem ameaças previamente desconhecidas, como *malwares zero-day* e ataques avançados de engenharia social. A engenharia de requisitos precisa incluir mecanismos que permitam ao *firewall* evoluir e atualizar suas regras de detecção com rapidez e eficácia [Soewito and Andhika 2019]. A inclusão de funcionalidades de aprendizado de máquina nos requisitos de *firewalls* pode ser uma solução para esse problema, permitindo que o sistema aprenda e se adapte a novos padrões de ataque automaticamente. No entanto, a implementação dessas tecnologias traz novos desafios de validação, como a necessidade de garantir que os algoritmos estejam otimizados para evitar falsos positivos e negativos, além de assegurar que o sistema continue eficiente à medida que lida com volumes crescentes de dados e ameaças mais complexas [Gadallah, Waheed G et al. 2024].

5. Proposta: *Framework* MORAIS

Nesta seção é apresentado o *framework* MORAIS, cujo objetivo principal é auxiliar na especificação e validação dos requisitos de segurança em NGFWs. O *framework* fornece um modelo que pode ser aplicado pelas equipes de desenvolvimento para estruturar e monitorar os requisitos de segurança de forma contínua, garantindo a adaptação a novas ameaças e a conformidade com regulamentações vigentes. O MORAIS é composto por seis pilares principais, ilustrados na Figura 1, os quais representam o ciclo completo necessário para a implementação e manutenção de um NGFW.

O *Framework* MORAIS é estruturado em cinco etapas fundamentais, nas quais os seus pilares são abordados: *Coleta de Especificações*, *Definição de Métricas de Desempenho*, *Validação de Conformidade com Regulamentações*, *Integração com outros Sistemas*

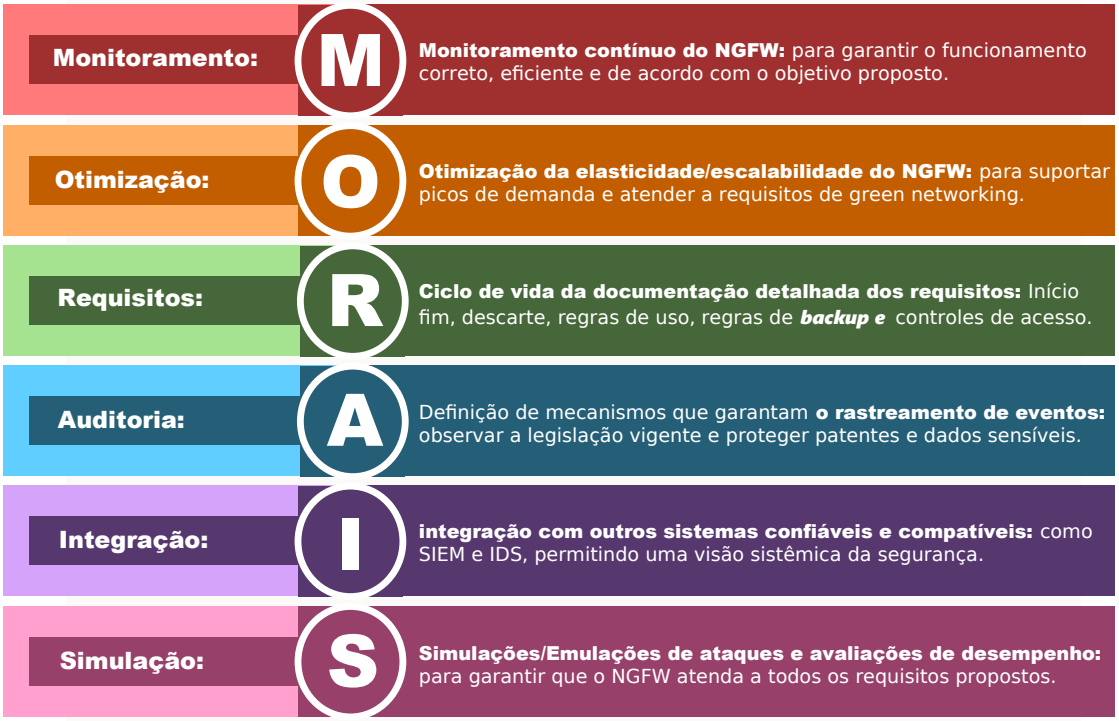

Figura 1. Framework MORAIS.

e *Supervisão Contínua*. Cada etapa é projetada para abordar desafios críticos previamente identificados. Tais etapas são abordadas nas subseções a seguir.

5.1. Coleta de Especificações

A primeira etapa, a *Coleta de Especificações* é crucial para o sucesso do *framework*. Esta etapa envolve um levantamento exaustivo e sistemático das necessidades de segurança da rede, abrangendo a identificação detalhada das especificações funcionais e não funcionais. Nesta fase, são considerados fatores como tipos de tráfego, potenciais vetores de ataque, políticas internas de segurança e regulamentações aplicáveis, incluindo a Lei Geral de Proteção de Dados (LGPD), no Brasil, e a GDPR, na Europa.

A participação ativa de todas as partes interessadas — engenheiros de segurança, desenvolvedores de sistemas, administradores de rede e gestores de conformidade — é essencial para garantir uma compreensão abrangente das especificações. Técnicas avançadas de elicitação, como entrevistas estruturadas, *workshops* colaborativos, análise de tarefas e modelagem de processos, devem ser empregadas para capturar todas as necessidades e restrições relevantes.

5.2. Definição de Métricas de Desempenho

A segunda etapa, a *Definição de Métricas de Desempenho*, concentra-se na determinação de parâmetros quantitativos que permitam avaliar o impacto das funcionalidades de segurança implementadas no desempenho global da rede. Essas métricas devem abranger indicadores como latência, largura de banda efetiva (*throughput*), taxa de perda de pacotes e utilização de recursos computacionais (*i.e.*, CPU e memória).

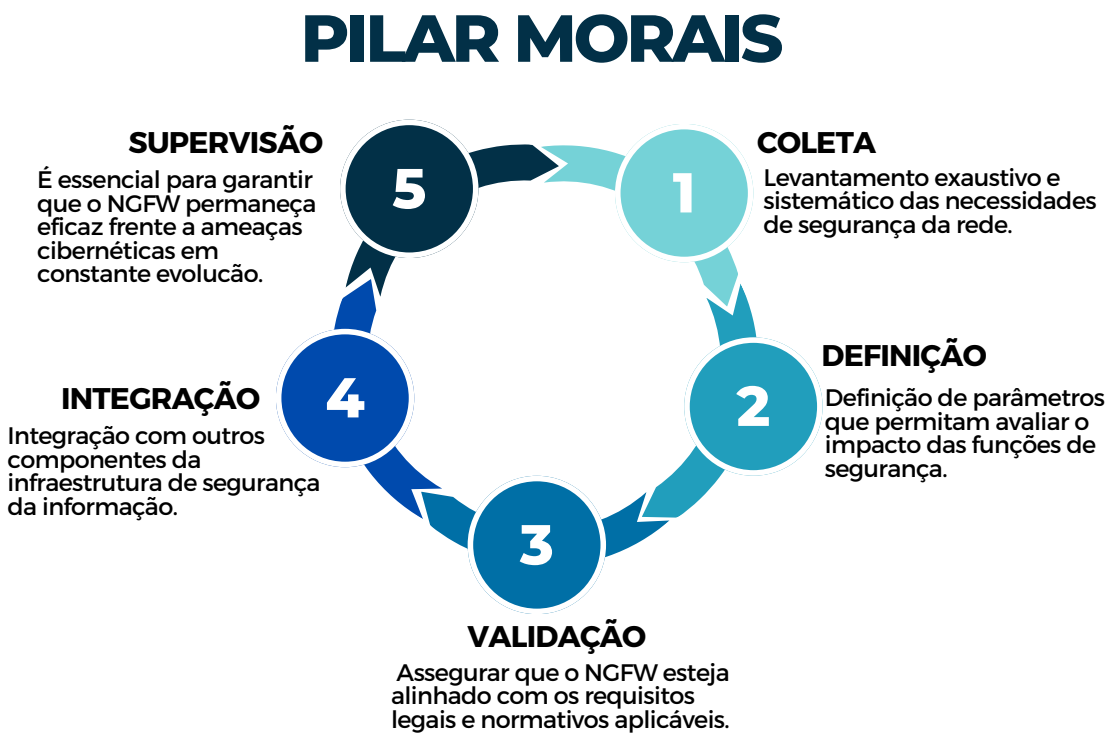

Figura 2. Implementação do *framework* MORAIS.

É fundamental que essas métricas sejam estabelecidas tanto para condições operacionais normais quanto para cenários de ataque simulados. Para isso, é imperativo o desenvolvimento de um conjunto robusto de testes de estresse e simulações de ataques cibernéticos, aplicáveis a diferentes cenários operacionais. Realizar esses testes em ambientes semi-reais — que replicam de forma fiel a infraestrutura de produção sem afetar diretamente o ambiente operacional real — é essencial para validar a eficácia e a resiliência do NGFW sob diversas condições. Essa abordagem permite identificar e corrigir vulnerabilidades e problemas de desempenho antes da implantação definitiva, garantindo que o sistema esteja adequadamente preparado para enfrentar ameaças reais.

5.3. Validação de Conformidade com Regulamentações

A terceira etapa, a *Validação de Conformidade com Regulamentações*, é dedicada a assegurar que o NGFW esteja alinhado com os requisitos legais e normativos aplicáveis, como a LGPD e GDPR. Portanto, os requisitos de conformidade legais que foram identificados na primeira etapa são verificados.

Ademais, nesta fase são definidos e implementados os mecanismos de auditoria, registro (*logging*) e rastreamento de dados necessários para garantir a transparência e a rastreabilidade das operações de segurança. A configuração adequada desses mecanismos é vital para possibilitar auditorias eficientes, facilitar a detecção e a resposta a incidentes de segurança e evitar violações de conformidade que possam resultar em penalidades legais e danos à reputação da organização e de seus usuários.

5.4. Integração com outros Sistemas

A quarta etapa, *Integração com outros Sistemas*, aborda a interoperabilidade do NGFW com outros componentes da infraestrutura de segurança da informação, tais como Sistemas de Gerenciamento de Informações e Eventos de Segurança (SIEM) e Sistemas de Detecção de Intrusões (IDS). A integração eficiente com esses sistemas permite a troca de informações em tempo real, possibilitando a correlação de eventos de segurança provenientes de múltiplas fontes. Isso aprimora significativamente a capacidade de detecção precoce de ameaças e a coordenação de respostas a incidentes, contribuindo para uma postura de segurança mais proativa e abrangente.

5.5. Supervisão Contínua

A etapa final, *Supervisão Contínua*, é essencial para garantir que o NGFW permaneça eficaz frente a ameaças cibernéticas em constante evolução. Esta supervisão envolve a atualização periódica das regras e políticas de segurança, bem como a implementação de técnicas avançadas, como algoritmos de aprendizado de máquina e análise comportamental, para a identificação proativa de padrões anômalos de tráfego e atividades suspeitas. Além disso, a supervisão contínua assegura que o NGFW se mantenha alinhado com quaisquer alterações nas regulamentações de proteção de dados, permitindo ajustes oportunos nas configurações e nos processos de conformidade.

5.6. Relação de Pilares e Implementação

Conforme abordado ao longo desta seção, a implementação do *framework* MORAIS se dá por meio do cumprimento de múltiplas etapas. A matriz MORAIS, ilustrada na Figura 2 faz o mapeamento dos pilares que são implementados em cada uma das etapas descritas.

6. Estudo de Caso

Para ilustrar a aplicação do *framework*, consideramos um estudo de caso baseado na implementação de um NGFW em uma grande empresa de telecomunicações, que enfrenta ataques emergentes e sofisticados nos dias atuais. Nesta organização, os principais desafios incluem a mitigação de ataques DDoS e a garantia de conformidade com a LGPD, exigindo soluções de segurança robustas e eficientes.

Na fase de elicitação de requisitos, foram identificadas ameaças como ataques volumétricos e tentativas de exploração de vulnerabilidades. Em resposta, os engenheiros definiram métricas de desempenho que garantiram que o NGFW pudesse lidar com altos volumes de tráfego sem comprometer a qualidade do serviço. Na fase de validação, a equipe de conformidade verificou que o *firewall* possuía todas as funcionalidades necessárias para coletar logs detalhados de incidentes e garantir a privacidade dos dados.

A integração com o SIEM da empresa permitiu uma análise centralizada de eventos de segurança, melhorando significativamente o tempo de resposta a incidentes. Por fim, o monitoramento contínuo assegurou a atualização do NGFW em tempo real para proteger a rede contra novas variantes de ataques, mantendo a conformidade com regulamentações emergentes.

Como resultado, o *framework* MORAIS demonstrou que a sua implementação em um cenário de prova de conceitos se mostrou bem-sucedida. Destaca-se que, além

da criação de um NGFW adequado, também foi promovida a criação de um ciclo de melhoria contínua. Ao abordar todos os aspectos críticos da definição e validação de requisitos de segurança, o *framework* MORAIS oferece uma solução abrangente para os desafios enfrentados durante o desenvolvimento de *firewalls* modernos. A aplicação do MORAIS em ambientes reais, como demonstrado no estudo de caso, destaca o seu potencial para contribuir na garantia da segurança e conformidade, mesmo em redes complexas e dinâmicas.

7. Conclusão

Este trabalho explorou um campo emergente ao abordar a especificação de requisitos de segurança em NGFWs, fornecendo direções iniciais para enfrentar os desafios dessa área. Através da proposta do *framework* MORAIS, foi possível delinear um conjunto de etapas estruturadas para guiar o desenvolvimento e a validação de requisitos de segurança em NGFWs, com foco no monitoramento contínuo, otimização, auditoria e integração com outros sistemas de segurança.

O estudo de caso ilustrativo demonstrou como o *framework* MORAIS pode ser aplicado em um cenário realista, proporcionando não apenas uma abordagem prática para lidar com ameaças dinâmicas, mas também assegurando conformidade com regulamentações em constante evolução. Para além do cenário avaliado, é importante observar que o MORAIS pode ser aplicado em qualquer contexto ou cenário que exija proteção contra ataques cibernéticos emergentes. Ademais, o MORAIS promove um ciclo de melhoria contínua, garantindo que os NGFWs sejam adaptáveis, eficientes e capazes de enfrentar os desafios emergentes.

Portanto, a implementação do *framework* MORAIS pode trazer benefícios significativos para as organizações que buscam fortalecer suas soluções de segurança, ao mesmo tempo em que mantém o desempenho de suas redes e a conformidade com as regulamentações de proteção de dados.

Como trabalhos futuros, está prevista a implementação do *framework* MORAIS em cenários práticos no contexto de ambientes reais. Com base nessa implementação, serão aprimorados todos os processos do MORAIS. Por fim, pretende-se desenvolver uma documentação detalhada sobre o *framework* proposto.

Referências

Abusamrah, I., Madhoun, A., and Iseed, S. (2021). Next-generation firewall, deep learning endpoint protection and intelligent SIEM integration. Technical report, Palestine Polytechnic University.

Ahmed, N. and Matulevicius, R. (2014). A Method for Eliciting Security Requirements from the Business Process Models. In *CAiSE*, volume 1164, pages 57–64.

Drkag, P. and Szymura, M. (2018). Technical and legal aspects of database's security in the light of implementation of general data protection regulation. In *CBU International Conference Proceedings...*, volume 6, page 156. Central Bohemia University.

Gadallah, Waheed G et al. (2024). A deep learning technique to detect distributed denial of service attacks in software-defined networks. *Computers & Security*, 137:103588.

Hamilton, Robert et al. (2020). Deep packet inspection in firewall clusters. In *2020 28th Telecommunications Forum (TELFOR)*, pages 1–4. IEEE.

Hussain, A. and Mkpojiogu, E. O. (2016). Requirements: Towards an understanding on why software projects fail. In *AIP Conference Proceedings*, volume 1761. AIP.

Hussain, S., Kamal, A., Ahmad, S., Rasool, G., and Iqbal, S. (2014). Threat modelling methodologies: a survey. *Sci. Int.(Lahore)*, 26(4):1607–1609.

Makhdoomi, A., Jan, N., Goel, N., et al. (2022). Conventional and next generation firewalls in network security and its applications. In *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, pages 964–969. IEEE.

Meridji, K., Al-Sarayreh, K. T., Abran, A., and Trudel, S. (2019). System security requirements: A framework for early identification, specification and measurement of related software requirements. *Computer Standards & Interfaces*, 66:103346.

Mishra, A. et al. (2024). Security requirements specification by formal methods: a research metadata analysis. *Multimedia Tools and Applications*, 83(14):41847–41866.

Morić, Z., Dakic, V., Djekic, D., and Regvart, D. (2024). Protection Of Personal Data In The Context Of E-commerce. *Journal of cybersecurity and privacy*, 4(3):731–761.

Nweke, Livinus Obiora et al. (2022). A LINDDUN-based privacy threat modelling for national identification systems. In *2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*, pages 1–8.

PMI (2010). Projects fail due to poor requirements management. Accessado: 22-09-2024.

Rajkumar, B. and Arunakranthi, G. (2023). Evolution for a secured path using nexgen firewalls. In *2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON)*, pages 1–6. IEEE.

Shaheed, A. and Kurdy, M. B. (2022). Web application firewall using machine learning and features engineering. *Security and Communication Networks*, 2022(1):5280158.

Singh, B. and Cheema, S. S. (2023). Next generation firewall and self authentication for network security. In *2023 Seventh International Conference on Image Information Processing (ICIIP)*, pages 707–713.

Soewito, B. and Andhika, C. E. (2019). Next generation firewall for improving security in company and iot network. In *2019 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, pages 205–209. IEEE.

Xiong, W. and Lagerström, R. (2019). Threat modeling–a systematic literature review. *Computers & security*, 84:53–69.