Gerenciamento Integrado e Adaptativo de Firewalls baseado na Fonte Única de Verdade (SSoT) da Rede

Jerônimo Menezes[1], **Leonardo Bitzki**[1], **Diego Kreutz**[1], **Rodrigo Brandão Mansilha**[1]

[1] Universidade Federal do Pampa (UNIPAMPA)

{jscmenezes,ljbitzki}@gmail.com

{diegokreutz,mansilha}@unipampa.edu.br

Resumo. *Este trabalho propõe uma arquitetura modular e adaptativa para o gerenciamento de firewalls, fundamentada no conceito de Fonte Única de Verdade (SSoT). A solução integra monitoramento, orquestração e aplicação de políticas de segurança em redes heterogêneas, permitindo respostas automatizadas a eventos operacionais e de segurança. Avaliações experimentais evidenciam a capacidade da arquitetura em reagir de forma ágil a mudanças na infraestrutura e mitigar ataques DoS com eficiência.*

1. Introdução

A gestão de firewalls em redes modernas impõe desafios técnicos e operacionais relevantes. Em ambientes heterogêneos, a diversidade de sintaxes e a ausência de controle centralizado dificultam a manutenção da consistência e aumentam a probabilidade de erros humanos, que figuram entre as principais causas de incidentes de segurança [Alicea and Alsmadi 2021, Bringhenti et al. 2024].

Diante desse cenário, cresce o interesse por soluções automatizadas que priorizem consistência, rastreabilidade e resposta em tempo real a eventos. O conceito de *Fonte Única de Verdade* (*Single Source of Truth* (SSoT)) tem ganhado destaque por centralizar o estado desejado da rede e viabilizar a orquestração automatizada de políticas de segurança.

Este trabalho apresenta o DynSecNet, uma solução aberta e modular para o gerenciamento adaptativo de firewalls baseada em SSoT. O DynSecNet integra monitoramento, tradução de políticas e aplicação em dispositivos, permitindo reações automáticas a eventos como alterações de serviços e alertas de segurança. Sua arquitetura é composta exclusivamente por software livre e possui potencial de compatibilidade com equipamentos de diferentes fabricantes.

As contribuições principais incluem:

- Modelo orientado por eventos com suporte a reações adaptativas;
- Integração nativa com a SSoT (NetBox), com rastreabilidade via *change logging*;
- Avaliação prática em dois cenários reais: ativação de serviço e mitigação de DoS, com tempo médio de reação inferior a dois segundos;
- Modelo operacional baseado em *templates*, *pipelines* automatizados (Ansible) e agentes de telemetria flexíveis.

Ao longo deste artigo, são apresentados os trabalhos relacionados, a arquitetura da ferramenta, suas principais funcionalidades e a demonstração de sua aplicabilidade por meio de casos práticos, incluindo uma comparação com soluções existentes.

2. Trabalhos Relacionados

Erros de configuração em firewalls permanecem entre as principais causas de falhas de segurança [Alicea and Alsmadi 2021]. Trabalhos recentes têm buscado mitigar essa complexidade por meio de automação, abstrações e orquestração.

O FWunify [Fiorenza 2021] propõe uma arquitetura modular com uma linguagem declarativa (FWlang) voltada para redes híbridas. O FireMason [Hallahan et al. 2017] utiliza exemplos positivos para gerar regras por meio de síntese programável. O SDFW [Chowdhary et al. 2018] explora firewalls distribuídos em redes SDN, com ênfase no controle de tráfego lateral. Linder et al. [Linder et al. 2024] aplicam automação com Nornir e o conceito de SSoT, com validação prévia e reconciliação de estado.

O uso de técnicas de inteligência artificial tem ampliado a adaptabilidade dos firewalls. Ahmad et al.[Ahmad 2025] e Duan et al.[Duan and Al-Shaer 2025] apresentam mecanismos de reconfiguração autônoma baseados em aprendizado de máquina. Bargury et al. [Bargury et al. 2017] demonstram que é possível derivar regras eficazes a partir de dados NetFlow e exemplos rotulados.

Revisões mais amplas [Islam et al. 2020] identificam três eixos centrais na orquestração de segurança: unificação, automação e execução coordenada. O paradigma de *Intent-Based Networking* (IBN) também tem sido explorado como forma de manter coerência entre as intenções declaradas e as políticas efetivamente aplicadas [Adeola Adewa et al. 2025, Clemm et al. 2022].

A Tabela 1 apresenta uma síntese das principais características das soluções analisadas. O DynSecNet se destaca por combinar todos os aspectos considerados desejáveis: integração com uma *Fonte Única de Verdade* (SSoT), comportamento adaptativo frente a eventos, rastreabilidade por meio de *change logging* e arquitetura modular com componentes substituíveis. Esses atributos posicionam a ferramenta como uma solução robusta, flexível e alinhada às demandas contemporâneas de gerenciamento seguro de políticas de firewall em ambientes de rede heterogêneos.

Tabela 1. Trabalhos relacionados

Solução	Fonte de Verdade	Adaptativo	Rastreabilidade	Modular
[Hallahan et al. 2017]	Não	Não	Não	Não
[Chowdhary et al. 2018]	Não	Parcial	Não	Parcial
[Ahmad 2025]	Não	Sim	Não	Não informado
[Fiorenza 2021]	Parcial	Não	Parcial	Sim
[Imoukhuede et al. 2025]	Sim	Não	Parcial	Parcial
DynSecNet	Sim	Sim	Sim	Sim

3. Modelo DynSecNet para Gerenciamento Adaptativo

O DynSecNet foi concebido como uma solução modular e extensível para orquestração de políticas de firewall em redes heterogêneas, com base em uma Fonte Única de Verdade (SSoT) e em eventos operacionais oriundos da própria infraestrutura. Esta seção descreve os principais blocos que compõem sua arquitetura e como eles interagem para garantir consistência, rastreabilidade e capacidade de adaptação.

3.1. Visão Geral da Arquitetura

A Figura 1 apresenta a visão geral da arquitetura do DynSecNet. Ela é estruturada como uma pilha de camadas funcionais que intermedeiam a interação entre a SSoT, os agentes externos que alteram o estado desejado da rede e os dispositivos de segurança que aplicam as políticas.

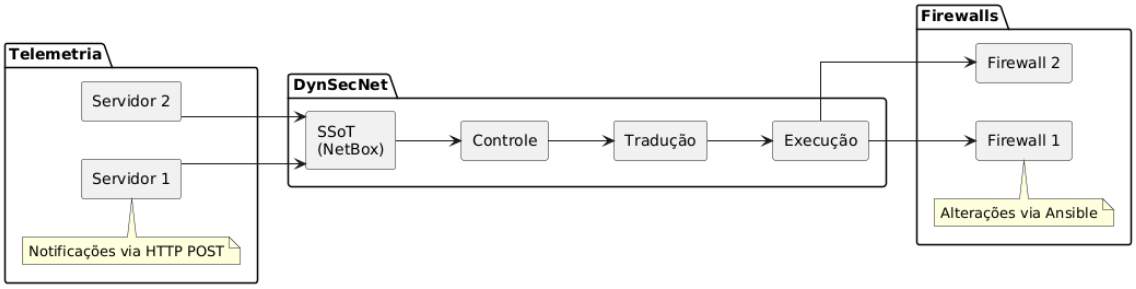

Figura 1. Arquitetura Geral do DynSecNet

A arquitetura parte do princípio de que qualquer componente da infraestrutura, como servidores de aplicação, sensores ou sistemas de monitoramento, pode notificar alterações operacionais por meio de requisições HTTP à SSoT. Essas modificações (por exemplo, a ativação de um novo serviço) são imediatamente detectadas pela Camada de Controle, que avalia o impacto sobre as políticas de segurança. A partir dessa análise, a Camada de Tradução gera as configurações específicas de firewall, que são repassadas à Camada de Execução para aplicação nos dispositivos. Esse encadeamento garante resposta adaptativa em tempo quase real, mantendo coerência com o estado desejado definido na SSoT.

3.2. Arquitetura em Camadas

A arquitetura do DynSecNet é composta por cinco camadas funcionais, cada uma representando uma responsabilidade-chave no fluxo de gerenciamento adaptativo de políticas de firewall. A primeira camada é a *Fonte Única de Verdade* (SSoT), que centraliza o estado desejado da rede, incluindo topologia, zonas, serviços e políticas de segurança — no sistema atual, o NetBox é utilizado como SSoT. A **Camada de Controle** atua como orquestrador logicamente centralizado, reagindo a alterações no estado desejado (geralmente oriundas de requisições HTTP POST) e acionando os fluxos de automação. A seguir, a **Camada de Tradução** converte abstrações declarativas em configurações específicas para os dispositivos, sendo implementada no protótipo por meio de templates Jinja2. A **Camada de Execução** é responsável por aplicar as configurações traduzidas, utilizando ferramentas como Ansible para garantir consistência e controle transacional. Por fim, os **Dispositivos de Infraestrutura** — como firewalls e roteadores — recebem as configurações geradas; a arquitetura do DynSecNet é agnóstica quanto à tecnologia utilizada, suportando iptables, nftables ou appliances comerciais. Esse modelo em camadas facilita a substituição, extensão ou reimplementação de partes do sistema com baixo acoplamento. Por exemplo, seria possível utilizar uma SSoT diferente do NetBox, como o phpIPAM, ou adotar outras ferramentas de execução como Netmiko em vez do Ansible. Essa modularidade também contribui para a adaptabilidade do sistema, permitindo que

diversos agentes (humanos ou automatizados) influenciem o comportamento da rede de forma coerente e auditável.

3.3. Modelo Operacional

O funcionamento do DynSecNet é orientado por eventos e baseado em pipelines automatizados que conectam a alteração no estado desejado da rede (registrado na SSoT) com a atualização do estado operacional nos dispositivos. A Figura 2 ilustra dois cenários representativos: a ativação de um novo serviço e a mitigação de um ataque de negação de serviço (DoS).

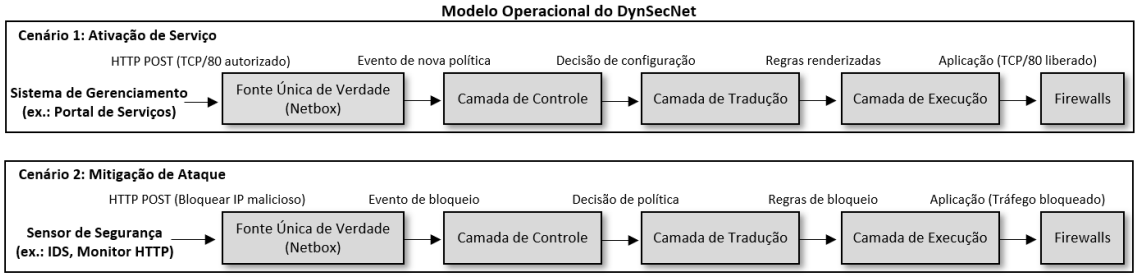

Figura 2. DynSecNet aplicado a dois cenários: (i) ativação de serviço e (ii) mitigação de ataque

No primeiro cenário, um sistema externo, como um portal de gerenciamento de serviços, envia uma requisição HTTP POST à SSoT (NetBox), indicando a ativação de um novo serviço na rede (por exemplo, liberação da porta TCP/80). Essa alteração no estado desejado dispara um evento interno capturado pela Camada de Controle do DynSecNet, que aciona o pipeline de automação. A configuração é traduzida para regras específicas pelo mecanismo de templates (Jinja2) e aplicada automaticamente nos firewalls usando Ansible, garantindo consistência e rastreabilidade.

No segundo cenário, um sensor de segurança (como um IDS ou script de monitoramento) detecta um tráfego anômalo originado de um endereço suspeito. Esse agente, de forma autônoma, realiza uma requisição HTTP POST que atualiza a SSoT com uma nova política de bloqueio. O mesmo ciclo de orquestração se repete, levando à reconfiguração automática dos dispositivos de segurança para mitigar o ataque, sem intervenção manual.

Esse modelo reforça a natureza adaptativa do DynSecNet: a integração com uma SSoT confiável permite que qualquer sistema autorizado, ao modificar o estado desejado via API, inicie um fluxo completo de reconfiguração da rede. A resposta a eventos operacionais e de segurança torna-se, assim, automatizada, rastreável e alinhada com as políticas definidas centralmente.

3.4. Diferenciais da Arquitetura DynSecNet

O DynSecNet se destaca por reunir, em uma mesma arquitetura, modularidade, reatividade e rastreabilidade. A separação entre as camadas de controle, tradução e execução facilita a manutenção e extensão da solução. A operação é orientada por eventos: alterações no estado desejado, registradas na SSoT, disparam fluxos automáticos de reconfiguração via APIs REST. Em termos de segurança, toda modificação é registrada no mecanismo de *change logging* da SSoT (NetBox), assegurando coerência entre o declarado e o aplicado. A solução é independente de fornecedor, compatível com múltiplos

firewalls (iptables, nftables, appliances), e baseada inteiramente em software livre, favorecendo sua adoção em contextos públicos e acadêmicos.

4. Avaliação Experimental

Esta seção apresenta uma avaliação da viabilidade prática do DynSecNet em dois cenários distintos: a ativação de um novo serviço e a mitigação de um ataque DoS. O objetivo é demonstrar a capacidade da solução em aplicar políticas de forma consistente e com baixa latência, a partir de mudanças no estado desejado registradas na SSoT.

4.1. Cenário 1: Ativação de Serviço

Neste experimento, simulamos a liberação de um serviço web (porta TCP/80) por meio da alteração do estado desejado na SSoT. A ação é realizada por um container NGINX que executa um `HTTP POST` para atualizar a política no NetBox. Essa modificação aciona, automaticamente, um fluxo de automação que traduz a política e aplica a regra no firewall. A Figura 3 ilustra esse ciclo completo, desde a alteração na SSoT até a aplicação nos dispositivos, evidenciando a reatividade do sistema baseada unicamente na atualização do estado desejado.

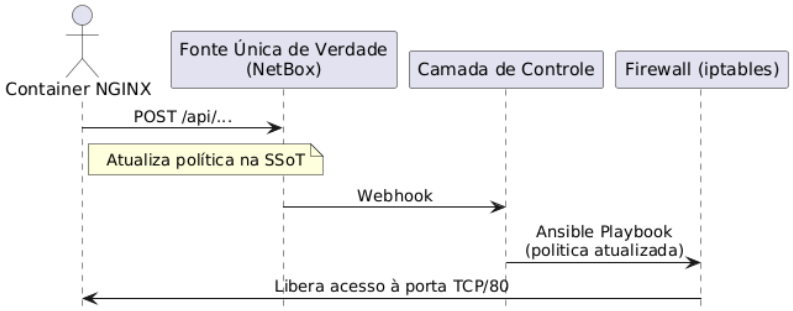

Figura 3. Fluxo de ativação automática de serviço via SSoT

Para avaliar o tempo de reação do sistema, foram coletados os timestamps do container responsável pela alteração e da aplicação efetiva da regra no firewall. Em cinco execuções consecutivas, o tempo médio registrado foi de aproximadamente 1,91 segundos, com variações entre 1,87s e 1,96s. Esses resultados demonstram a capacidade do DynSecNet de responder de forma rápida e autônoma a mudanças no estado desejado da rede, validando sua proposta de reatividade e rastreabilidade.

4.2. Cenário 2 – Mitigação de Ataque DoS

Este cenário avalia a capacidade do DynSecNet de mitigar automaticamente um ataque de negação de serviço (DoS) identificado por sensores externos à arquitetura. O objetivo é bloquear rapidamente o tráfego de origem maliciosa, minimizando o impacto sobre a infraestrutura da rede.

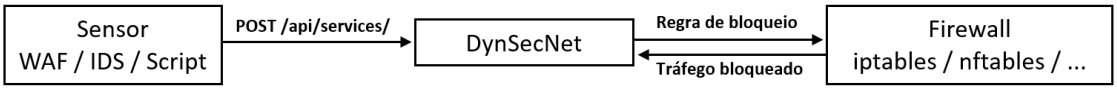

Figura 4. Fluxo de mitigação de ataque DoS via DynSecNet

A Figura 4 ilustra o fluxo operacional envolvido. Um sensor (como um WAF, IDS ou script customizado) detecta o ataque e realiza uma requisição HTTP POST para a API da SSoT, atualizando o estado desejado da rede com a inclusão de uma regra de bloqueio. Essa modificação dispara o pipeline de automação, que aplica imediatamente a nova política nos dispositivos de firewall. A resposta é registrada na própria SSoT, garantindo rastreabilidade completa do processo.

Os testes foram realizados com tráfego de ataque simulado, gerado a partir de um contêiner configurado para enviar requisições repetidas a um servidor web. O tempo total de mitigação foi calculado como a diferença entre o instante de detecção e o momento em que o tráfego foi efetivamente bloqueado pelo firewall. A Figura 5 apresenta os tempos observados.

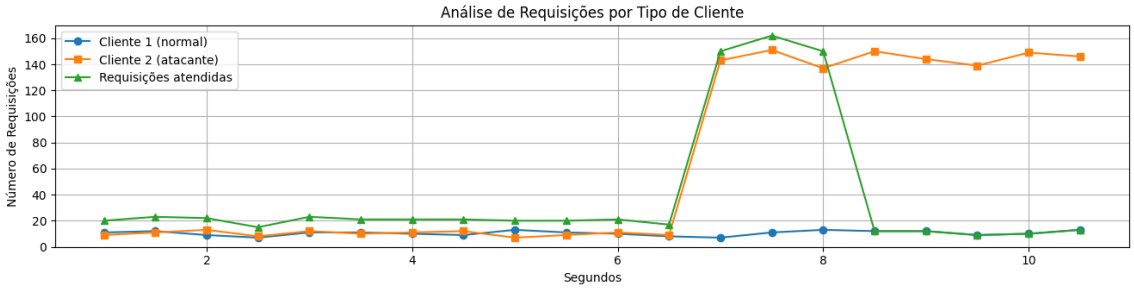

Figura 5. Fluxo de ativação automática de serviço via SSoT

Os dados confirmam a capacidade do DynSecNet de mitigar ataques de forma eficaz e com baixa latência, mantendo a rede protegida com mínima intervenção humana. O ciclo completo, da detecção ao bloqueio, ocorre de forma automática e com rastreabilidade garantida, reforçando a proposta de uma orquestração de segurança baseada em estado desejado.

5. Considerações Finais e Trabalhos Futuros

Este trabalho apresentou o DynSecNet, uma arquitetura modular e adaptativa para o gerenciamento de firewalls, baseada no conceito de *Fonte Única de Verdade* (SSoT). A solução integra monitoramento, orquestração e aplicação de políticas em redes heterogêneas, promovendo consistência entre o estado desejado e o estado operacional. Os experimentos demonstraram a capacidade da ferramenta em reagir a eventos críticos com baixa latência e mínima intervenção humana.

A integração com a SSoT possibilita automação eficaz e rastreabilidade completa. A separação em camadas favorece a extensibilidade, permitindo a inclusão de novos tradutores e mecanismos de aplicação. No entanto, a centralização impõe desafios relacionados à resiliência, e ainda não foram explorados mecanismos proativos para antecipação de incidentes.

Entre as direções futuras, destacam-se: (i) a incorporação de técnicas de IA generativa e aprendizado por reforço; (ii) o suporte a redes emergentes, como 5G/6G e ambientes industriais; e (iii) a verificação formal de políticas em contextos com modificações simultâneas.

O DynSecNet está disponível como projeto de código aberto[1] e segue em evolução para aplicação em redes acadêmicas, de pesquisa e de provedores de acesso.

Agradecimentos. A pesquisa contou com apoio da CAPES (Código de Financiamento 001) e da FAPERGS, por meio dos termos de outorga 24/2551-0001368-7 e 24/2551-0000726-1.

Referências

Adeola Adewa, Vincent Anyah, Omoniyi David Olufemi, Adedeji Ojo Oladejo, and Toluwanimi Olaifa (2025). The impact of intent-based networking on network configuration management and security. *Global Journal of Engineering and Technology Advances*, 22(1):063–068.

Ahmad, T. (2025). AI-Driven Dynamic Firewall Optimization Using Reinforcement Learning for Anomaly Detection and Prevention.

Alicea, M. and Alsmadi, I. (2021). Misconfiguration in Firewalls and Network Access Controls: Literature Review. *Future Internet*, 13(11):283.

Bargury, M., Levin, R., and Ronen, R. (2017). Learning to Customize Network Security Rules.

Bringhenti, D., Marchetto, G., Sisto, R., and Valenza, F. (2024). Automation for Network Security Configuration: State of the Art and Research Trends. *ACM Computing Surveys*, 56(3):1–37.

Chowdhary, A., Huang, D., Alshamrani, A., Sabur, A., Kang, M., Kim, A., and Velazquez, A. (2018). SDFW: SDN-based Stateful Distributed Firewall.

Clemm, A., Ciavaglia, L., Z. Granville, L., and Tantsura, J. (2022). Intent-Based Networking - Concepts and Definitions. Technical Report RFC9315, RFC Editor.

Duan, Q. and Al-Shaer, E. (2025). Firewall Regulatory Networks for Autonomous Cyber Defense.

Fiorenza, M. M. (2021). Gerenciamento de firewalls em redes híbridas.

Hallahan, W. T., Zhai, E., and Piskac, R. (2017). Automated repair by example for firewalls. In *2017 Formal Methods in Computer Aided Design (FMCAD)*, pages 220–229, Vienna. IEEE.

Imoukhuede, A. B., Sheltami, T. R., Mahmoud, A. H., and Barnawi, A. Y. (2025). Optimization of network device hardening in a multivendor environment. *Scientific Reports*, 15(1):15042.

Islam, C., Babar, M. A., and Nepal, S. (2020). A Multi-Vocal Review of Security Orchestration. *ACM Computing Surveys*, 52(2):1–45.

Linder, S., Lisetska, P., and Stutz, R. (2024). *Network Configuration Automation with Infrahub and Nornir*. other, OST Ostschweizer Fachhochschule.

[1] `https://github.com/SBSeg25/DynSecNet`