Gerenciamento de Conexões usando Firewall Automatizado a partir de Dados de Inteligência sobre Ameaças

Marcus A. S. Costa[1], Yago M. da Costa[1], Douglas. A. Silva[1], Ariel L. Portela, Rafael L. Gomes[1]

[1]Universidade Estadual do Ceará (UECE), Brasil.

{marcus.costa,yago.costa,aguiar.pimenta}@aluno.uece.br,

rafa.lopes@uece.br

Resumo. *Em um contexto de ameaças cibernéticas em constante evolução, a necessidade de soluções de segurança dinâmicas e adaptativas é imperativa, onde a abordagem de Inteligência sobre Ameaças Cibernéticas visa coletar, analisar e interpretar informações relevantes sobre ameaças digitais. Dentro deste contexto, este artigo apresenta uma solução de segurança chamada FIBRA (Firewall Integrado com Blacklists e Reputação Automatizado), projetada para gerenciar conexões em infraestruturas de rede a partir de Dados de Inteligência sobre Ameaças. O FIBRA visa combater autonomamente as ameaças através de atualizações em tempo real das blacklists e técnicas de filtragem, enquanto alcança uma escalabilidade adequada e fornece uma visão abrangente do tráfego de rede e ameaças identificadas. Experimentos realizados a partir de uma infraestrutura de nuvem real indicam a eficácia do FIBRA na identificação e mitigação de conexões suspeitas, contribuindo significativamente para a segurança de redes em ambientes complexos e dinâmicos.*

Abstract. *In a context of constantly evolving cyber threats, the need for dynamic and adaptive security solutions is imperative, where the approach of Threat Intelligence, which aims to collect, analyze, and interpret relevant information about digital threats, is crucial. Within this context, this article presents a security solution called FIBRA (Integrated Firewall with Automated Blacklists and Reputation), designed to manage connections in network infrastructures based on Cyber Threat Intelligence data. FIBRA aims to autonomously combat threats through real-time updates of blacklists and filtering techniques while achieving adequate scalability and providing a comprehensive view of network traffic and identified threats. Experiments conducted in a real cloud infrastructure indicate the effectiveness of FIBRA in identifying and mitigating suspicious connections, contributing to network security in complex and dynamic environments.*

1. Introdução

No cenário digital em constante evolução de hoje, a segurança da informação não é apenas uma necessidade, mas uma prerrogativa para proteger dados sensíveis contra o crescente volume e sofisticação dos ataques cibernéticos. Esta realidade exige soluções de segurança que sejam adaptáveis, resilientes e capazes de antecipar ameaças emergentes [Silveira et al. 2023, Aguiar et al. 2011], principalmente na tarefa de gerenciamento de conexões de rede. O gerenciamento de conexões de rede refere-se ao con-

trole e supervisão do tráfego de rede entre dispositivos para garantir a segurança, desempenho e disponibilidade da rede, além de otimizar o uso dos recursos disponíveis [Portela et al. 2024, Gomes et al. 2016, Gomes et al. 2010].

A integração de tecnologias avançadas e estratégias proativas é essencial para manter a integridade, a confidencialidade e a disponibilidade dos dados [Portela et al. 2023]. A aplicação de um firewall responsivo, que se adapta dinamicamente para bloquear endereços IP de baixa reputação com base em análises de reputação e comportamento, é uma resposta inovadora a essa necessidade, destacando uma evolução na forma como as redes podem ser protegidas.

Outro mecanismo que faz com que a funcionalidade e a eficácia da segurança da rede sejam aprimoradas significativamente é Inteligência sobre Ameaças Cibernéticas (*Threat Intelligence*), também conhecida como inteligência de ameaças ou ciberinteligência, que é um campo que se dedica a coletar, analisar e interpretar informações relevantes sobre ameaças e atividades maliciosas no ambiente digital [Wagner et al. 2019]. Uma das ações dessa abordagem é a aplicação de registros de conexão e técnicas de geolocalização de IP faz parte dessa abordagem. Estes não só ajudam na identificação de fontes de tráfego potencialmente maliciosas, como também permitem uma análise geográfica detalhada das tentativas de acesso, oferecendo uma perspectiva valiosa sobre as origens dos ataques. Este aspecto é crucial para a implementação de medidas de segurança mais direcionadas e eficazes, como enfatizado por [Komosny 2023], e permite uma resposta mais precisa às ameaças.

Além disso, a capacidade de responder automaticamente a ameaças identificadas é crucial na proteção de redes [Lopes Gomes and Roberto Mauro Madeira 2012]. A automação permite uma ação rápida e eficaz, essencial em um ambiente onde cada segundo conta. As técnicas de análise de fluxos de logs em tempo real, destacadas por [Yadav and Mishra 2023], e os sistemas de filtragem automática de pacotes, ilustrados por [Rizkilina and Rosyid 2022], são exemplos de como a tecnologia pode ser utilizada para reforçar a segurança. Estas estratégias garantem que o sistema de firewall não apenas identifique, mas também reaja proativamente a ameaças emergentes, baseado nos registros de conexão e identificação de comportamentos ”não esperados”, fortalecendo a rede contra invasões. Adicionalmente, o conceito de *blacklists* e a gestão da reputação de IPs são fundamentais para o fortalecimento da segurança de redes, onde as *blacklists* públicas, que catalogam endereços IP conhecidos por atividades maliciosas, são uma ferramenta valiosa para a pré-filtragem de tráfego potencialmente perigoso.

Essa abordagem é reforçada pela aplicação de técnicas TARPIT (*Hiding Computer Network Proactive Security Tools Unmasking Features*), uma técnica defensiva que, ao invés de bloquear completamente o acesso, degrada a conexão, desestimulando atividades maliciosas sem negar o acesso aos serviços. Contudo, atualmente, estas abordagens conceituais mencionadas (Inteligência sobre Ameaças, TARPIT, resposta automatizada, etc) para gerenciamento de conexões são realizadas por equipes de cibersegurança, que analisam, de forma manual ou semi-automatizada, os dados coletados para identificar ameaças emergentes, vulnerabilidades exploradas, identidades de atores maliciosos e quaisquer outras informações relevantes [Afzaliseresht et al. 2020, Vielberth et al. 2019]. Desta forma, faz-se necessário desenvolver soluções de segurança que consigam automatizar o processo de análise de ameaças e automatização, incluindo aspectos de eficiência,

escalabilidade e tempo de resposta.

Dentro deste contexto, este artigo apresenta uma solução de segurança, chamada FIBRA (Firewall Integrado com Blacklists e Reputação Automatizado), projetada para gerenciar conexões em infraestruturas de rede a partir de Dados de Inteligência sobre Ameaças. O FIBRA visa combater autonomamente as ameaças através de atualizações em tempo real das *blacklists* e técnicas de filtragem, enquanto alcança uma escalabilidade adequada e fornece uma visão abrangente do tráfego de rede e ameaças identificadas. O FIBRA, através do firewall automatizado, gerencia as conexões que acessam a infraestrutura de rede, ou seja, ele analisa as informações, bloqueando, degradando ou habilitando a troca de informações desta, enquanto o processo de reputação com dados de inteligência sobre ameaças é realizado. Experimentos realizados, a partir de uma infraestrutura de nuvem real, indicam a eficácia do FIBRA na identificação e mitigação de conexões suspeitas, contribuindo significativamente para a segurança de redes em ambientes complexos e dinâmicos. Os resultados indicam uma eficácia notável na identificação de conexões suspeitas e na prevenção de ataques cibernéticos.

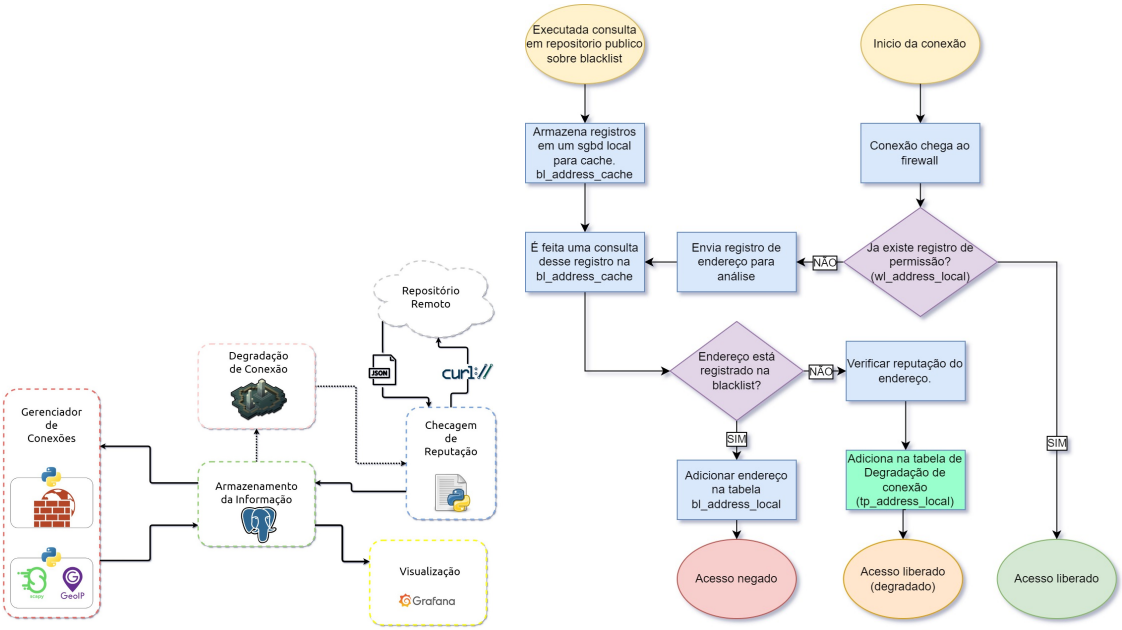
O FIBRA avança o estado da arte, pois as soluções existentes não consideram bases de dados de ameaças a fim de implantar uma solução adaptável às ameaças. Dentre esses trabalhos relacionados, pode-se destacar as referências [Yang and Lim 2021], [Lazar et al. 2021], [Tosun et al. 2021] e [Wang et al. 2020] que apresentam soluções para identificação de ameaças com abordagens reativas e baseadas em somente dados locais, limitando sua aplicabilidade em cenários complexos. Portanto, a solução proposta neste artigo oferece uma abordagem alternativa às existentes na literatura, incorporando *Threat Intelligence* de forma mais integrada com múltiplas fontes de dados. Além disso, ao aplicar um Firewall automatizado, a solução proposta tem a capacidade de se adaptar a cenários dinâmicos e levar em conta um espectro mais diversificado de características e comportamentos de atividades maliciosas.

2. Proposta

Este artigo apresenta o desenvolvimento e a solução *FIBRA* (Firewall Integrado com Blacklists e Reputação Automatizado), um sistema avançado de segurança destinado à infraestrutura de redes, principalmente em redes empresariais que possuem diversas conexões. O sistema representa uma evolução em relação aos firewalls tradicionais, incorporando um mecanismo dinâmico de atualização de *blacklists* e avaliação de reputação IP para aprimorar continuamente sua capacidade de detecção e mitigação de ameaças.

O procedimento empregado no desenvolvimento do sistema de firewall automatizado com integração de *blacklists*, dados de base de ameaças e técnica de TARPIT foi estruturado para abordar tanto o design teórico quanto a implementação prática do sistema. A implementação prática enfatizou o uso de tecnologias de contêineres e Interfaces de Aplicação (*APIs*) para garantir a escalabilidade, a portabilidade e a eficiência da solução. Foram desenvolvidos alguns módulos, ilustrados na Figura 1(a), incluindo a detecção de conexões, armazenamento de dados, consulta a *blacklists*, análise de comportamento, aplicação de degradação de conexão, gerenciamento de firewall e visualização de dados. Cada módulo foi projetado para operar de forma integrada, formando um sistema coeso. Assim, os seguintes módulos foram definidos:

- Gerenciador de Conexões: visa monitorar e analisar o tráfego de rede em tempo real



(a) Organização dos módulos. (b) Fluxo de Execução.

Figura 1. Visão Geral do FIBRA

para identificar padrões ou comportamentos suspeitos que possam indicar atividades maliciosas. Na implementação realizada, utiliza-se o Scapy[1] para capturar conexões TCP do tipo SYN, filtrando e registrando informações relevantes, incluindo a tentativa de geolocalização usando a base da MaxMind[2].

- Checagem de Reputação: tem por objetivo consultar as bases de ameaças as tentativas de conexão capturadas pelo módulo Gerenciador de Conexões. Assim, este emprega requisições para consultar endereços IP em *blacklists* de repositórios remotos (tais como a plataforma *AbuseIPDB*[3]), visando identificar e marcar IPs de baixa reputação. De maneira geral, verifica-se se um endereço IP está listado em alguma *blacklist* ou possui má reputação, para decisão de alimentação da tabela de TARPIT.
- Degradação de Conexão: Configuração de regras para responder a IPs identificados como maliciosos, incluindo a geração de *TCP-reset* para IPs em *blacklists* e a limitação de taxa de conexões para IPs não listados.
- Armazenamento de Dados: Tem como objetivo principal registrar e armazenar informações relacionadas a eventos de segurança detectados pela solução, atuando como uma abordagem de consulta rápida para verificações já realizadas (otimizando o tempo de resposta), bem como base de informações para o módulo de visualização.
- Visualização de Dados: Interface gráfica para leitura e visualização dos dados coletados, facilitando a análise de padrões e a tomada de decisão.

O fluxo de execução, descrito na Figura 1(b), garante uma abordagem sistemática para a detecção, análise e resposta a ameaças de segurança. O fluxo da informação ocorre da seguinte forma: Um módulo realiza o download da blacklist para armazenamento local,

[1]https://scapy.net/
[2]https://www.maxmind.com/
[3]https://www.abuseipdb.com/

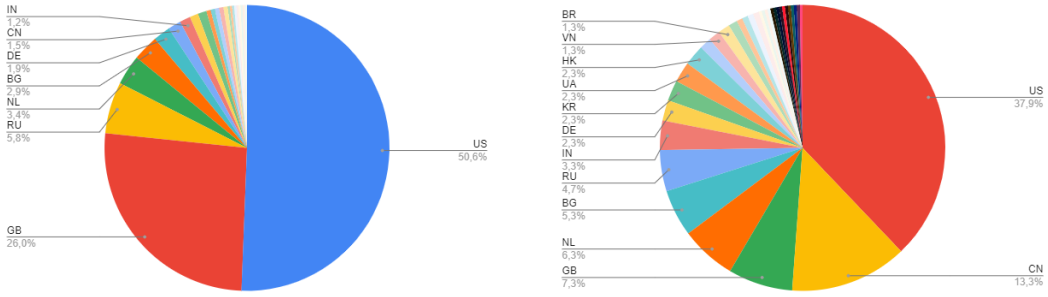
gerando um cache dos dados. Em paralelo, o módulo de escuta registra as conexões TCP do tipo SYN, concatena com a lista de geolocalização e armazena em banco. Após esse registro, um outro módulo compara os dados armazenados pelo módulo de escuta com o cache da blacklist local e, em seguida, realiza a consulta via API desse endereço para coletar sua reputação e pontuação de confidencialidade. Nesse momento, caso o endereço esteja no cache da blacklist, ele será adicionado à tabela de bloqueio. Caso não esteja nesse registro, sera adicionado à tabela de degradação de conexão.

De maneira geral, o FIBRA aplica uma metodologia que combina diversas abordagens cruciais para soluções de segurança (fontes de inteligência de ameaças, TARPIT, ações automatizadas, etc.), com um foco especial na utilização de dados dinâmicos. Esta metodologia visa alcançar uma detecção mais precisa de tentativas de conexão que podem ser uma ameaça para os dispositivos e serviços em execução sobre a infraestrutura de rede, contribuindo assim para uma prestação de serviços mais segura e robusta para as empresas e instituições.

3. Experimentos e Análise de Desempenho

Nesta seção, apresentamos uma análise detalhada das conexões identificadas e gerenciadas pelo sistema FIBRA, ressaltando sua capacidade de detecção e ação sobre atividades potencialmente maliciosas. A avaliação foi realizada com base em duas tabelas principais: `bl_address_local` e `tp_address_local`, que registram as conexões identificadas como pertencentes a *blacklists* e as encaminhadas para degradação, respectivamente.

A tabela `bl_address_local` contém registros das conexões que foram identificadas como maliciosas e correspondem a endereços IP presentes nas *blacklists*. Esses dados indicam que uma proporção significativa das conexões de *blacklist* originou-se dos Estados Unidos e da Grã-Bretanha. A distribuição geográfica das detecções sugere que o sistema FIBRA está ativamente identificando e respondendo a ameaças de diversas origens internacionais, destacando sua eficácia global.



(a) Conexões Identificadas na Blacklist. (b) Conexões Não Identificadas na Blacklist.

Figura 2. Resultados

Na tabela `tp_address_local`, que rastreia as conexões não reconhecidas completamente mas suspeitas o suficiente para serem degradadas. Interessantemente, as conexões provenientes dos Estados Unidos representam o maior volume de tráfego sujeito à degradação. Isso pode refletir uma estratégia defensiva efetiva contra ataques automatizados de alta frequência, típicos de bots ou scanners de rede, que frequentemente originam-se ou são roteados através dos EUA. Os resultados apresentados reforçam a funcionalidade do sistema FIBRA como uma ferramenta proativa de segurança de rede.

A identificação eficiente de conexões de *blacklist* e a subsequente degradação do tráfego suspeito são cruciais para mitigar o risco antes que ataques mais sérios se concretizem. Adicionalmente, os dados de degradação mostram que o FIBRA pode efetivamente aplicar medidas preventivas sem a necessidade de bloquear completamente os endereços IP, o que poderia resultar em interrupção de serviços para usuários legítimos.

A partir dos experimentos realizados, percebe-se que o FIBRA possui a capacidade de identificar e gerir conexões potencialmente maliciosas, utilizando uma metodologia focada em *blacklists* atualizadas e a técnica de TARPIT para degradação de tráfego. A vasta gama de incidências detectadas, espalhadas por uma diversidade geográfica, destaca a eficácia do sistema em um cenário global de segurança cibernética. Além disso, considerando a importância da velocidade de resposta em segurança cibernética, o desenvolvimento de mecanismos automatizados de atualização e adaptação das *blacklists* é uma característica crucial para a aplicabilidade em cenários reais, possibilitando que a solução não apenas reaja às ameaças conhecidas, mas também se adapte proativamente às ameaças emergentes globais.

4. Conclusão

Em um cenário de ameaças cibernéticas em constante evolução, a necessidade de soluções de segurança dinâmicas e adaptativas é crucial. Nesse contexto, a abordagem de Inteligência sobre Ameaças Cibernéticas, que busca coletar, analisar e interpretar informações relevantes sobre ameaças digitais, torna-se fundamental. Assim, este artigo introduz uma solução de segurança denominada FIBRA, desenvolvida para gerenciar conexões em infraestruturas de rede utilizando dados de Inteligência sobre Ameaças. O FIBRA tem como objetivo combater ameaças de forma autônoma, por meio de atualizações em tempo real das listas de bloqueio (blacklists) e técnicas de filtragem avançadas.

Como trabalhos futuros, pretende-se evoluir a solução para integrar técnicas de ciência de dados e Inteligência Artificial de forma automatizada no fluxo de execução, permitindo indicativos mais robustos para a solução e, consequentemente, oferecer um suporte mais eficaz às equipes de segurança para lidar com incidentes de segurança.

Agradecimentos

Os autores agradecem ao CNPq (N^o 303877/2021-9 e N^o 405940/2022-0) e a CAPES (N^o 88887.954253/2024-00) pelo apoio financeiro.

Referências

Afzaliseresht, N., Miao, Y., Michalska, S., Liu, Q., and Wang, H. (2020). From logs to stories: Human-centred data mining for cyber threat intelligence. *IEEE Access*, 8:19089–19099.

Aguiar, E. S., Pinheiro, B. A., Figueirêdo, J. F. S., Cerqueira, E., Abelém, A. J. G., and Gomes, R. L. (2011). Trends and challenges for quality of service and quality of experience for wireless mesh networks. *Wireless Mesh Networks*, pages 127–148.

Gomes, R., Junior, W., Cerqueira, E., and Abelem, A. (2010). A qoe fuzzy routing protocol for wireless mesh networks. In Zeadally, S., Cerqueira, E., Curado, M., and Leszczuk, M., editors, *Future Multimedia Networking*, pages 1–12, Berlin, Heidelberg. Springer Berlin Heidelberg.

Gomes, R. L., Bittencourt, L. F., Madeira, E. R., Cerqueira, E., and Gerla, M. (2016). A combined energy-bandwidth approach to allocate resilient virtual software defined networks. *Journal of Network and Computer Applications*, 69:98–106.

Komosny, D. (2023). Evidential value of country location evidence obtained from ip address geolocation. *PeerJ Comput Sci.*

Lazar, D., Cohen, K., Freund, A., Bartik, A., and Ron, A. (2021). Imdoc: Identification of malicious domain campaigns via dns and communicating files. *IEEE Access*, 9:45242–45258.

Lopes Gomes, R. and Roberto Mauro Madeira, E. (2012). A traffic classification agent for virtual networks based on qos classes. *IEEE Latin America Transactions*, 10(3):1734–1741.

Portela, A. L., Menezes, R. A., Costa, W. L., Silveira, M. M., Bittecnourt, L. F., and Gomes, R. L. (2023). Detection of iot devices and network anomalies based on anonymized network traffic. In *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, pages 1–6.

Portela, A. L. C., Ribeiro, S. E. S. B., Menezes, R. A., de Araujo, T., and Gomes, R. L. (2024). T-for: An adaptable forecasting model for throughput performance. *IEEE Transactions on Network and Service Management*, pages 1–1.

Rizkilina, T. M. and Rosyid, N. R. (2022). Packet filtering automation system design based on data synchronization on ip profile database using python. *Journal of Internet and Software Engineering (JISE)*, 3:12–19.

Silveira, M. M., Portela, A. L., Menezes, R. A., Souza, M. S., Silva, D. S., Mesquita, M. C., and Gomes, R. L. (2023). Data protection based on searchable encryption and anonymization techniques. In *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, pages 1–5.

Tosun, A., De Donno, M., Dragoni, N., and Fafoutis, X. (2021). Resip host detection: Identification of malicious residential ip proxy flows. In *2021 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–6.

Vielberth, M., Menges, F., and Pernul, G. (2019). Human-as-a-security-sensor for harvesting threat intelligence. *Cybersecurity*, 2:1–15.

Wagner, T. D., Mahbub, K., Palomar, E., and Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers Security*, 87:101589.

Wang, Q., Li, L., Jiang, B., Lu, Z., Liu, J., and Jian, S. (2020). Malicious domain detection based on k-means and smote. In *Computational Science–ICCS 2020: 20th International Conference, Amsterdam, The Netherlands, June 3–5, 2020, Proceedings, Part II 20*, pages 468–481. Springer.

Yadav, M. and Mishra, D. S. (2023). Identification of network threats using live log stream analysis. In *2023 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing (PCEMS)*, pages 1–6.

Yang, J. and Lim, H. (2021). Deep learning approach for detecting malicious activities over encrypted secure channels. *IEEE Access*, 9:39229–39244.