NAMEDZEUS – UM SISTEMA DE IMPOSIÇÃO DE POLÍTICAS DE REDE BASEADO EM HOST

CHIANFA, Murilo de Araújo[1]; COELHO, Fabrício José[2]; ; MODESTO, Lisandro Rogério; RANDO,Déverson Rogério

Palavras-chave: Firewall. Netfilter. Iptables.

INTRODUÇÃO

O ambiente corporativo é um ambiente que integra diversos sistemas de diferentes organizações, sendo a rede a tecnologia utilizada para realizar a integração que permite todas as conexões entre seus elementos. A confiabilidade, integridade e disponibilidade da rede são essenciais para o próprio negócio da organização.

Os seguintes fatores justificam a preocupação com a segurança contínua: a natureza dos ataques, novas vulnerabilidades das tecnologias emergentes, a criação de novas formas de ataques, o aumento da conectividade, a complexidade da defesa, o aumento dos crimes digitais e os grandes prejuízos ocasionados pela falta de segurança. (NAKAMURA; GEUS, 2003, p.10).

Uma organização pode se proteger utilizando diferentes técnicas e mecanismos, um deles é o que vamos abordar aqui, o firewall de redes. Firewall é um ponto entre duas ou mais redes, por onde todo o tráfego transita por sua estrutura, permitindo assim um controle e auditoria de maneira eficaz.

---

[1] Murilo de Araujo Chianfa. Acadêmico do Curso de Bacharelado em Sistemas de Informação da faculdade de Apucarana – FAP. Apucarana – Pr. 2023.

[2] Fabrício José Coelho. Docente/Orientador do Curso de Bacharelado em Sistema de Informação da Faculdade de Apucarana – FAP. Apucarana – PR. 2023.

Porém de acordo com as recomendações do Instituto Nacional de Padrões e Tecnologia (NIST, 2009, p.20, tradução nossa), os firewalls como gateway da rede por si só, não são capazes de reconhecer todas as instâncias e formas de ataques, permitindo que alguns ataques penetrem e alcancem os hosts internos, e os ataques enviados de um host interno para outro podem nem passar pelo firewall principal, sendo necessário a adição de outros firewalls pelo caminho, como por exemplo os firewalls baseados em host para os servidores de aplicação, fornecendo assim uma camada adicional de segurança contra os ataques pela rede.

Para João Eriberto (2013, p.353): “Com a defesa em profundidade, não dependeremos de somente um mecanismo de segurança. Teremos, em vez disso, vários mecanismos que se ligam uns aos outros e a falha de um desses mecanismos não compromete todo o conjunto.”

OBJETIVO

Tendo em vista a grande complexidade no gerenciamento das regras e políticas do firewall para os diversos hosts, o software desenvolvido visa sanar esta dor agrupando essas regras em grupos para serem de forma centralizada, associadas aos servidores hospedando serviços de mesmo propósito.

> A complexidade das regras de filtragem cresce cada vez mais na medida em que serviços e aplicações são adicionados no ambiente corporativo. Dessa forma, o gerenciamento centralizado se torna um fator importante para que erros na criação e implementação de regras sejam minimizados (ESQUIVEL, 2006, p.29).

O sistema terá um conjunto de regras já pré cadastradas para que o administrador de redes possa ter um norte na configuração e customização das políticas e regras a serem aplicadas aos seus servidores.

Contando ainda com a possibilidade de realizar uma auditoria nas mudanças aplicadas aos servidores, para que seja possível rastrear quaisquer alterações.

MÉTODO

Inicialmente foi realizada uma pesquisa literária sobre o assunto para o embasamento teórico dos requisitos funcionais. Em conjunto a isso, a construção dos diagramas foi iniciada, tanto o diagrama de casos de uso, quanto o diagrama de modelo de entidade e relacionamento para o banco de dados.

Após o término do levantamento de requisitos e da criação dos diagramas foi dado início à construção do projeto. Para dar início, foi escolhido utilizar um template pronto para a interface gráfica, para facilitar e agilizar o desenvolvimento do software.

DESENVOLVIMENTO

Para o desenvolvimento do software em questão, foi dedicada uma atenção primordial aos aspectos relacionados à segurança. Compreendendo a importância crítica de garantir sua integridade e proteção, uma abordagem meticulosa na concepção e elaboração do sistema foi necessária, com práticas de codificação segura, a fim de prevenir potenciais vulnerabilidades, atualizações regulares ao longo do desenvolvimento e mecanismos de proteção nas funcionalidades mais importantes.

A linguagem de programação escolhida para a construção do software foi PHP com o framework Laravel, já para o banco de dados, foi utilizado MariaDB, Apache2 para o servidor WEB, Nginx como proxy reverso, RabbitMQ para enfileiramento dos alertas, Rsyslog como coletor dos pacotes maliciosos, Redis2 para cache em memória primária, Docker para o empacotamento da aplicação e C++ com o framework Drogon para a criação da probe.

Todas as tecnologias utilizadas estão em sua última versão estável disponível, garantindo assim uma maior estabilidade e performance para o sistema.

CONCLUSÕES

Atualmente o sistema está com seu MVP (Minimum viable product) pronto e agora passa pela fase final de testes antes de seu lançamento oficial, com uma arquitetura sólida e funcionalidades inovadoras, o mesmo se destaca como uma solução abrangente e eficaz para o que se propõe.

Outro destaque notável é a capacidade de integrar-se perfeitamente em diferentes distribuições linux, evidenciando sua versatilidade e adaptabilidade. Com uma interface intuitiva e ferramentas de gerenciamento simplificadas proporcionam uma experiência de usuário otimizada, reduzindo o tempo de aprendizado e aumentando a eficiência operacional.

Após o término dos testes finais, o próximo passo será lançar o software ao público para assim validar sua eficácia, o software desenvolvido será comercializado por meio de um modelo de licenciamento flexível, que por sua vez, se adapta às necessidades e ao porte de diferentes organizações.

A transparência e a flexibilidade do modelo de venda, irão assegurar que o software atenderá às expectativas e requisitos individuais de cada cliente,

promovendo assim uma parceria duradoura e confiável.

Fonte: Autoria própria, 2023.

REFERÊNCIAS

NAKAMURA, GEUS. **Segurança de Redes em Ambientes Cooperativos**. 2ª. ed., São Paulo, Futura, 2003.

NIST - National Institute of Standards and Technology. **Recommendations of the National Institute of Standards and Technology**. 1ª. ed., Gaithersburg, 2009.

MOTA, João E. **Análise de Tráfego em Redes TCP/IP: Utilize tcpdump na análise de tráfegos em qualquer sistema operacional**. 1ª ed., Novatec Editora, 2013.

ESQUIVEL, C.J. **Gerenciamento de regras de Firewall IPTABLES em ambiente Linux**. 2006.