FAVENI

FACULDADE VENDA NOVA DO IMIGRANTE

PÓS-GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

FERMYNO BRAGA GUTIERREZ

ESTUDO DE CASO SOBRE O USO DO SISTEMA PFSENSE COMO SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO

PORTO ALEGRE / RS

2022

TÍTULO DO TCC: ESTUDO DE CASO SOBRE O USO DO SISTEMA PFSENSE COMO SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO

Declaro que sou autor deste Trabalho de Conclusão de Curso**.** Declaro também que o mesmo foi por mim elaborado e integralmente redigido, não tendo sido copiado ou extraído, seja parcial ou integralmente, de forma ilícita de nenhuma fonte além daquelas públicas consultadas e corretamente referenciadas ao longo do trabalho ou daqueles cujos dados resultaram de investigações empíricas por mim realizadas para fins de produção deste trabalho.

Assim, declaro, demonstrando minha plena consciência dos seus efeitos civis, penais e administrativos, e assumindo total responsabilidade caso se configure o crime de violação aos direitos autorais.

RESUMO - Diante do cenário da pandemia do COVID-19 foi observado um crescimento exponencial do uso da Internet. Nesse sentido, observa-se o surgimento de novas ameaças informáticas, requerendo que as organizações revisem com grande frequência suas políticas de segurança de informação. Entretanto, observa-se com preocupação de que muitas organizações não adotam adequadas soluções de segurança, resultando em redes corporativas inseguras e vulneráveis às ameaças digitais. Diante disso, aumenta a necessidade da utilização de *firewalls*, visando permitir um controle mais apurado sobre as ameaças digitais. O presente estudo, realizado na forma de Estudo de Caso descritivo e exploratório, visa analisar a implantação do *firewall* pfSense, através de informações que abordam os recursos e debilidades da sua utilização na instituição estudada. O resultado do estudo evidenciou que o *firewall* pfSense mostrou-se uma solução apropriada para facilitar a gestão dos processos de segurança, e proteger a rede corporativa de ameaças externas.

PALAVRAS-CHAVE: *Firewall* pfSense. *Ameaças informáticas*. Segurança da Informação.

1 INTRODUÇÃO

Diante do cenário da pandemia do COVID-19 foi observado um crescimento exponencial do uso da Internet, tanto no aumento do número de usuários, como na ampliação da presença digital de organizações de todos os portes. Nesse sentido, observa-se o surgimento de novas ameaças informáticas, requerendo que as organizações revisem com grande frequência suas políticas de segurança de informação. Entretanto, observa-se com preocupação de que muitas organizações não adotam adequadas soluções de segurança.

Diante desse cenário, o presente estudo propõe a utilização do *firewall* pfSense como solução adicional de segurança digital, e visa responder a seguinte problemática investigativa: “Em que medida a implantação de uma solução de *firewall* pfSense incrementará os níveis de segurança da rede corporativa da organização estudada?”

Ao longo das próximas páginas, o presente estudo evidenciará que o *firewall* pfSense permite reduzir grande parte dos incidentes relacionados com as ameaças informáticas.

O presente estudo possui como objetivo geral: explanificar sobre a efetividade do pfSense em incrementar a segurança informática na organização estudada. Os objetivos específicos passam por realizar um levantamento bibliográfico acerca das informações relacionadas com o tema; e implementar a solução de *firewall* pfSense visando ampliar o nível de segurança da rede corporativa da organização estudada.

Entende-se que o trabalho apresentado justifica-se pelo grau de facilidade da implantação do *firewall*, da sua versatilidade de uso em um grande leque de organizações, e devido a sua confiabilidade, robustez, e baixo custo total.

O presente estudo será desenvolvido na forma de Estudo de Caso descritivo e exploratório, buscando analisar a implantação e utilização do pfSense, através de observações que evidenciem os benefícios e dificuldades da sua utilização na organização objeto deste estudo.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 AMEAÇAS, RISCOS E VULNERABILIDADES EM SISTEMAS INFORMÁTICOS

É notório que a Internet representa um leque de oportunidades para muitas empresas, entretanto, é preciso ter em mente de que, por se tratar de uma rede pública, as organizações estão expostas aos riscos de ataques informáticos que podem invadir sistemas corporativos visando a obtenção de informações sigilosas de forma ilícita.

De forma abrangente, podemos representar as redes informáticas como um conjunto de equipamentos interconectados entre si (computadores, impressoras, telefones celulares, etc.). Tanenbaum e Wetherall (2012) relacionam as diferentes formas de conexão informática, tais como: cabos de cobre, microondas, raios infravermelhos, fibras óticas, satélites de comunicação, entre outros.

Diante desse contexto, podemos entender como vulnerabilidade o grau de insegurança que cada dispositivo conectado a uma rede apresenta, sejam eles: computadores, servidores, routers, entre tantos outros. E, muitas vezes, são essas vulnerabilidades que podem dar origem a diversos ataques informáticos. Tarazona (2007) observa que podemos agrupar as ameaças informáticas em quatro grandes categorias: fatores humanos; falhas de segurança nos sistemas de informações; desastres naturais; e atos maliciosos.

As técnicas de ataques informáticos, utilizados por *hackers* ou grupos criminosos, estão cada vez mais sofisticadas e visam explorar as vulnerabilidades dos sistemas informáticos. Somado a isso, observa-se que muitos usuários desconhecem a gravidade dos riscos que estão envolvidos no acesso de *sites* inapropriados, ou mesmo quando realizam o *download* (transferência de arquivos para o computador) de aplicações de origens duvidosas, que podem roubar informações sigilosas, ou mesmo, comprometer o funcionamento de todo o sistema.

2.2 A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

É importante frisar que mesmo as mais avançadas técnicas e ferramentas de segurança de informação não garantem que os sistemas informáticos estejam totalmente seguros. A segurança das redes corporativas é de suma importância, para evitar que seja colocada em risco a exposição de informações sensíveis, a integridade dos dados, ademais dos prejuízos legais e financeiros resultantes do vazamento de dados.

Nessa linha de pensamento, Ferreira e Araújo (2008) destacam que o tema Segurança da Informação ganhou relevância no contexto corporativo, como fruto dos processos de informatização. Corroborando esse pensamento, Pérez e Merino (2008) ressaltam que a segurança da informação é uma temática que busca proteger a integridade e privacidade das informações armazenadas em sistemas informáticos.

Diante do exposto, verifica-se que a administração das ameaças informáticas ultrapassa os equipamentos e sistemas, abrangendo o estabelecimento de um apropriado sistema de controle de políticas, procedimentos, treinamentos, práticas, e a criação de uma estrutura que protega os ativos digitais de uma organização.

Nos dias atuais, os profissionais das tecnologias da informação podem contar com uma série de ferramentas que buscam ampliar a segurança dos sistemas informáticos, entre eles podemos citar o *software* antivírus, *Firewall*, e *softwares* adicionais (*antispyware*, *antimalware*, etc.).

Nesse contexto, é relevante destacar a importância do *firewall* na proteção e controle dos sistemas informáticos, sendo considerado como uma ferramenta quase obrigatória no desenho de soluções de segurança da informação.

2.3 O *FIREWALL* COMO FERRAMENTA DE PROTEÇÃO INFORMÁTICA

Podemos considerar um *firewall* como um dispositivo de segurança que inspecciona todo e qualquer fluxo de dados informáticos que circula em uma rede, definindo de acordo com certos critérios se permite ou bloqueia a passagem desses dados.

Em outras palavras, um *firewall* funciona como uma barreira que fica entre a rede informática interna, onde estão as informações que queremos proteger, e a rede exterior (como a Internet, por exemplo). Desse modo, o *firewall* busca assegurar que as ameaças externas não tenham acesso às informações privadas, além de evitar que ocorram diversos danos aos equipamentos de rede e sistemas informáticos da organização.

Uma analogia muito utilizada para representar a figura de um *firewall* é entender esse dispositivo como se fosse um vigilante que controla todo o fluxo de pessoas, confirmando se os mesmos não portam objetos suspeitos. Quando alguma forma de ameaça é detectada, o vigilante impedirá a entrada do suspeito no recinto.

Acompanhando esse pensamento, Kurose e Ross (2013) destacam que um *firewall* é um dispositivo que integra *hardware* e *software*, permitindo isolar uma rede interna de outra rede externa, bloqueando e habilitando a passagem de determinados tipos de dados.

Entretanto, para controlar efetivamente todo e qualquer fluxo de dados, o *firewall* necessita ser configurado respeitando um grupo definido de regras que permitam filtrar todo o tráfego que circula na rede, conforme critérios previamente definidos. Desse modo, o *firewall* pode converter-se em um componente fundamental na primeira linha de defesa dos sistemas informáticos, ampliando substancialmente a proteção dos dados que circulam no ambiente corporativo.

2.4 CONCEITOS BÁSICOS SOBRE O PFSENSE

Conforme sua página oficial na Internet, o pfSense é uma distribuição FreeBSD (sistema operacional de código aberto do tipo UNIX) especificamente concebida para a sua utilização como *firewall*. Ao longo de muitos anos, o FreeBSD foi considerado o sistema operacional mais seguro do mundo (FreeBSD, 2022). O pfSense é reconhecido pela sua facilidade de operação, visto que pode ser completamente administrado através de uma interface *web*.

Adicionalmente, cabe destacar que o pfSense é um produto reconhecido pela qualidade e baixo custo, visto que é totalmente gratuito, mesmo possuindo uma grande variedade de recursos e características comparáveis à grande maioria dos *firewalls* comerciais.

Entre os recursos mencionados podemos citar como funcionalidades do pfSense:

- *Firewall*,
- NAT (*Network Address Translation*),
- Alta Disponibilidade,
- VPN (*Virtual Private Network*),
- Servidor DNS,
- Servidor DHCP, entre outras.

Nesse sentido, Delfino (2020) destaca que o pfSense é uma solução muito robusta e largamente utilizada, principalmente nas redes informáticas. O *site* oficial ainda destaca que o pfSense é um sistema com mais de 1.000.000 de *downloads* e utilizado nas mais diversas organizações, desde soluções domésticas, até grandes corporações (pfSense, 2022).

3 METODOLOGIA

O presente trabalho se desenvolverá no formato de estudo de caso descritivo e exploratório, buscando relacionar, de forma não estatística, dados quantitativos a respeito da temática apresentada.

O presente estudo investigativo será realizado da forma descritiva, posto que serão observadas e descritas as características e vantagens do *firewall* pfSense como solução de segurança, bem como expor suas debilidades, dentro do contexto da organização objeto deste estudo.

O campo de estudo será uma empresa que atua no ramo de educação, com sede no sul do país. Por questões de privacidade, o nome da empresa não será mencionado no presente trabalho.

4 ANÁLISE DOS DADOS

4.1 APRESENTAÇÃO DA ORGANIZAÇÃO ESTUDADA

A organização objeto do presente estudo é uma empresa que atua no ramo da educação, com sede na região sul do país. Com o advento da pandemia do COVID-19, e a consequente popularização do *E-learning*, a instituição de ensino foi impelida a conceber uma estrutura para disponibilizar acesso aos cursos de maneira *online* aos seus alunos.

Entretanto, como de costume em muitas organizações, as políticas de segurança de informação da instituição não lograram avançar na mesma rapidez do surgimento de novas ameaças informáticas. Nesse sentido, a instituição, optou por contratar o serviço de hospedagem da plataforma educacional, terceirizando a segurança informática da plataforma e garantindo uma segurança adicional aos cursos disponibilizados.

Entretanto, a terceirização não contemplou a rede interna da organização. Como os colaboradores utilizam a Internet para executar as atividades rotineiras da instituição educativa, a organização dispõe de uma conexão à Internet através de fibra ótica, contratada junto à um provedor local de telecomunicações.

A instalação e configuração de todos os equipamentos de comunicação relacionados com a contratação do serviço de Internet ficaram a cargo do provedor, todavia, a estrutura disponibilizada, apesar de satisfatória para assegurar a comunicação com a rede mundial de computadores, está longe de contemplar uma solução verdadeiramente robusta de *firewall*. A solução final resultou em uma rede desprotegida e com poucas defesas perante a um ataque informático.

Em um cenário onde a organização faz uso das tecnologias da informação como elemento fundamental de seus processos operacionais, observa-se a obrigatoriedade de proteger o fluxo de informações que circulam na rede corporativa. Nesse sentido, a implantação de um dispositivo de *firewall* possibilitará monitorar os *websites* acessados, impossibilitando que os colaboradores acedam a conteúdos em desacordo com a política da organização, ou mesmo que coloque em risco a integridade da rede interna.

4.2 ANÁLISE DA IMPLANTAÇÃO DO *FIREWALL* PFSENSE

Visando controlar e reduzir as ameaças que podem acarretar em graves prejuízos para a instituição estudada, em particular no tocante aos riscos de invasão e roubo de informações, o presente estudo tratou da implantação de uma solução de segurança informática baseada no *firewall* pfSense.

Diante das inúmeras opções disponíveis no mercado, por uma série de fatores, foi realizada a escolha pelo pfSense. Entre os principais fatores considerados podemos citar o reduzido custo relacionado com a implementação do projeto, a robustez e estabilidade da solução apresentada, o grande número de funcionalidades disponíveis pelo pfSense, e principalmente a capacidade do pfSense em funcionar em

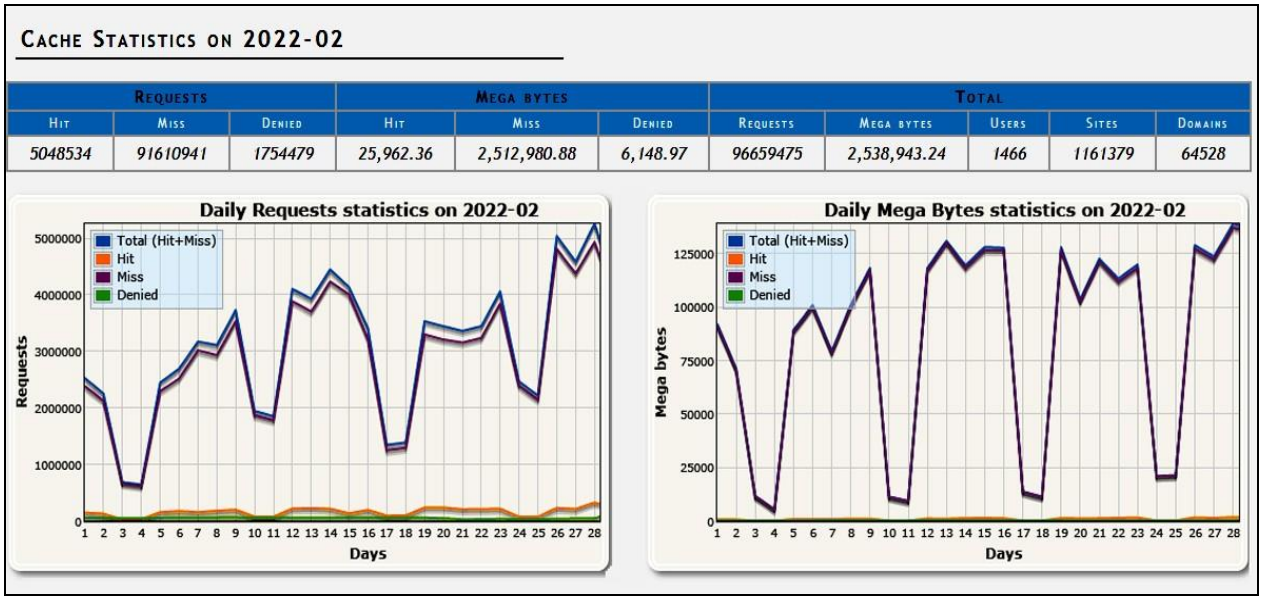
equipamentos com modestos requisitos de *hardware*, reduzindo o custo total da solução proposta.

A implantação da solução ocorreu rapidamente e sem transtornos. Como *hardware*, foi utilizado um computador que não estava mais em uso e que foi disponibilizado pela instituição. Embora obsoleto para os padrões atuais, o computador utilizado mostrou-se perfeitamente adequado para a operação do pfSense.

Na continuidade, foram realizados ajustes e otimizações no sistema, sendo possível observar, já nos primeiros dias, que a solução apresentada permitiu um controle mais apurado sobre os dados que circulam na rede corporativa, operando como uma barreira de proteção, entre os dados internos e as ameaças externas.

Uma das funcionalidades muito utilizada foi o SquidGuard, um redirecionador de URL que permite o controle de conteúdo dos sites e que pode ser facilmente integrado ao pfSense (SquidGuard, 2022). Através dele, foi possível configurar um servidor *proxy* que aumentou a velocidade de acesso à Internet, através do uso de *cache*, ademais da utilização de “listas negras” que permitiram filtrar *sites* perigosos.

Figura 1 - Relatório de requisições diárias na rede.



Fonte: Captura dos relatórios de acesso (2022).

Foi possível observar que a implantação de um servidor *firewall,* desde que seguindo critérios bem estruturados, possibilita preservar as informações críticas de uma organização. A solução apresentada permitiu, não apenas reduzir os incidentes de segurança da informação, mas também, permitiu uma adequada gestão dos dados que ingressam e saem da rede corporativa, bem como dos recursos computacionais envolvidos no processo.

5 CONSIDERAÇÕES FINAIS

Ao longo do presente estudo foi possível constatar que entende-se como pertinente a implantação de uma solução de segurança composta pelo *firewall* pfSense, visando monitorar, controlar, e manter a integridade da informação que transita na rede corporativa da instituição estudada, protegendo-a de ataques informáticos externos.

No caso estudado, foi possível monitorar e auditar a utilização da rede corporativa, bloqueando ameças informáticas e *sites* em desacordo com a política de segurança proposta. Adicionalmente, foi possível detectar tentativas de invasão ao siste ou de acessos não autorizados que foram bloqueados pelo pfSense e que, em momento algum, afetaram o funcionamento da rede interna.

Desse modo, o estudo respondeu de forma afirmativa a problemática investigativa proposta e que guiou o presente estudo, ou seja, a solução de *firewall* pfSense mostrou-se compatível com o propósito de assegurar a funcionalidade da rede interna, facilitando a gestão das políticas de segurança da informação, e blindando a rede corporativa de riscos e ameaças externas.

6 REFERÊNCIAS BIBLIOGRÁFICAS

DELFINO, Pedro. PfSense – **Principais vantagens e recursos dessa poderosa ferramenta de firewall.** Disponível em <https://e-tinet.com/linux/pfsense-vantagens/> Acesso em: 21 mar. 2022.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio. **Manual de Políticas de Segurança da Informação - Guia Prático para elaboração e implantação**. Rio de Janeiro: Ciência Moderna, 2008.

FREEBSD. **Resources for Newbies**. Disponível em: < https://www.freebsd.org/projects/newbies/>. Acesso em: 25 mar. 2022.

KUROSE, Jim; ROSS, Keith. **Redes de Computadores e a Internet: uma abordagem topdown**. 6. Ed. São Paulo: Addison Wesley, 2013.

PÉREZ P., J; MERINO, María. (2008). **Definición de seguridad informática. Definicion**. Disponível em: <https://definicion.de/seguridad-informatica/>. Acesso em: 04 abr. 2022.

PFSENSE. **Getting Started**. Disponível em: < https://www.pfsense.org/getting-started/>. Acesso em: 18 mar. 2022.

SQUIDGUARD. **SquidGuard Blacklists**. Disponível em: < http://www.squidguard.org/blacklists.html>. Acesso em: 19 mar. 2022.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de Computadores**. 5. ed. São Paulo: Pearson, 2012. 563 p. (2).

TARAZONA, Cesar. (2007). **Amenazas informáticas y seguridad de la información.** Derecho Penal Y Criminología. Disponível em: <https://revistas.uexternado.edu.co/index.php/derpen/article/view/965>.
Acesso em: 22 mar. 2022.