FAVENI

FACULDADE VENDA NOVA DO IMIGRANTE

PÓS-GRADUAÇÃO EM ENGENHARIA DE SOFTWARE

FERMYNO BRAGA GUTIERREZ

ESTUDO DE CASO SOBRE A IMPLANTAÇÃO DE FIREWALL PFSENSE EM UMA EMPRESA DO RAMO HOTELEIRO

PORTO ALEGRE / RS

2021

TÍTULO DO TCC: ESTUDO DE CASO SOBRE A IMPLANTAÇÃO DE FIREWALL PFSENSE EM UMA EMPRESA DO RAMO HOTELEIRO

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 - A segurança da informação é uma temática de grande preocupação no dia-a-dia das organizações, entretanto, muitas empresas contam com recursos limitados e não adotam soluções adequadas, resultando em redes inseguras e vulneráveis às ameaças digitais. Nesse sentido, cresce a importância da utilização de *firewalls* nas redes corporativas, permitindo um maior controle sobre as ameaças informáticas. O presente estudo será realizado na forma de Estudo de Caso descritivo e exploratório, visando descrever a utilização do *firewall* pfSense, através de análises que evidenciem os recursos e debilidades da sua utilização na empresa objeto de estudo. O resultado final mostrou que a solução de *firewall* pfSense mostrou-se apropriada em assegurar a funcionalidade da rede corporativa, facilitando a gestão dos processos de segurança, e protegendo-a de ameaças externas.

PALAVRAS-CHAVE: *Firewall* pfSense. *Software* Livre. Segurança da Informação.

1 INTRODUÇÃO

Nos dias atuais, vivemos em uma sociedade cada vez mais conectada, onde uma infinidade de informações sensíveis circula através da Internet. Nesse contexto, a segurança da informação é um tema de grande preocupação nas organizações, na medida em que a proteção dos dados deixou de ser uma preocupação secundária, para transformar-se em uma obrigatoriedade ética e legal.

Diante disso, cresce a importância da utilização de *firewalls* nas redes corporativas, permitindo um maior controle sobre as ameaças informáticas. Entretanto, muitas organizações contam com recursos limitados e não adotam soluções adequadas, resultando em redes inseguras e vulneráveis às ameaças digitais.

O presente estudo pretende propor a utilização do *firewall* de código aberto pfSense, devido ao seu elevado prestígio e reduzido custo de implantação, e pretende responder a seguinte problemática investigativa: “Em que medida a implantação de um *firewall* pfSense permitirá incrementar os níveis de segurança da rede informática da empresa estudada?”

Ao longo deste estudo, se demonstrará que o pfSense é um *firewall* de baixo custo, e que cumpre com o propósito de solucionar muitos dos problemas relacionados com as ameaças e vulnerabilidades das redes informáticas empresariais.

O presente trabalho tem como objetivo geral: identificar a eficácia do *firewall* pfSense em aumentar a segurança informática na rede empresarial da empresa estudada. Os objetivos específicos são: fazer um levantamento bibliográfico sobre informações pertinentes ao tema; e implementar o *firewall* pfFSense para aumentar o grau de segurança da rede da empresa estudada.

Entende-se que o presente levantamento justifica-se pela facilidade de implantação da solução apresentada em uma infinidade de organizações, devido a sua robustez, confiabilidade, eficiência e baixo custo.

O presente estudo será realizado na forma de Estudo de Caso descritivo e exploratório, visando descrever a utilização do *firewall* pfSense, através de análises que evidenciem os recursos e debilidades da sua utilização na empresa objeto de estudo.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 RISCOS E AMEAÇAS INFORMÁTICAS

A Internet universalizou o acesso às informações e abriu um leque de oportunidades para muitas organizações. Entretanto, por se tratar de uma rede pública, está exposta ao ataque de *hackers* e grupos criminosos que buscam invadir sistemas corporativos com a finalidade de obter informações sigilosas de forma ilícita.

De forma geral, pode-se entender como redes informáticas um conjunto de equipamentos (computadores, impressoras, telefones celulares, etc.) interconectados entre si. Nesse sentido, Tanenbaum e Wetherall (2012) ressaltam que existem várias formas de conexão informática, tais como: cabos de cobre, fibras óticas, microondas, raios infravermelhos, satélites de comunicação, entre outros. Essa miríade de possibilidades resulta em que, muitas vezes, os usuários mais leigos não tenham consciência de que seus dispositivos, ao estarem conectados por *wifi* ou *bluetooth*, por exemplo, estejam expostos aos perigos da rede mundial de computadores.

Nesse contexto, vulnerabilidade pode ser entendida como o grau de debilidade intrínseco a cada dispositivo conectado a uma rede, sejam eles: computadores, routers, servidores, entre tantos outros. Essas vulnerabilidades, por sua vez, podem dar origem a diversos ataques informáticos. Tarazona (2007) defende que podemos agrupar as ameaças informáticas em quatro grandes categorias: fatores humanos; falhas de segurança nos sistemas de informações; desastres naturais; e atos maliciosos.

Os ataques informáticos estão cada vez mais sofisticados e buscam explorar essas vulnerabilidades. Como agravante, grande parte dos usuários desconhece os riscos que estão associados ao acesso de sites inapropriados, ou quando realizam o *download* de aplicações duvidosas, que podem comprometer o funcionamento do equipamento, ou mesmo, roubar informações sigilosas do sistema.

2.2 SEGURANÇA DA INFORMAÇÃO

Mesmo fazendo uso das mais avançadas técnicas e ferramentas, é muito difícil garantir que os sistemas informáticos estejam totalmente seguros, independente do tamanho da organização. A proteção das redes corporativas é um tema de grande importância, na medida em que coloca em risco a integridade dos dados, exposição de informações sensíveis, além de prejuízos resultantes de uso inadequado dos recursos computacionais.

Nesse sentido, Ferreira e Araújo (2008) ressaltam que o tema Segurança da Informação ganhou importância no contexto organizacional, como resultado dos processos de informatização. Seguindo a mesma linha, Pérez e Merino (2008) salientam que a segurança da informação é uma disciplina que se encarrega de proteger a integridade e privacidade da informação armazenada em um sistema informático.

Observa-se que o processo de administração dos riscos informáticos vai além dos equipamentos e sistemas, incluindo a implantação de um apropriado sistema de controle de políticas, práticas, procedimentos e estruturas que visam proteger os ativos físicos e intelectuais de uma organização.

Atualmente, destaca-se a existência de inúmeras ferramentas que visam ampliar a segurança dos sistemas, entre eles: Antivírus, *Firewall*, e *softwares* adicionais (*antispyware*, *antimalware*, etc.). Nesse contexto, o *firewall* é considerado como uma ferramenta quase obrigatória na proteção e controle dos sistemas informáticos.

2.3 FIREWALL

Firewall pode ser entendido como um dispositivo de segurança que monitora todo o tráfego de dados que entra e sai em uma rede informática, decidindo, de acordo com critérios estabelecidos, se permite ou bloqueia cada dado que transita na rede.

Basicamente, funciona como uma barreira entre a rede interna, onde estão as informações sensíveis, e a rede externa, como a Internet, por exemplo. Ele protege os equipamentos de rede das ameaças externas que podem roubar informações privadas e confidenciais, além de ocasionar diversos danos aos sistemas informáticos.

Através de uma analogia, podemos entender a figura do *firewall* como um vigilante que controla todo o tráfego de pessoas, verificando se os mesmos não portam armas ou objetos suspeitos. Ao detectar algum tipo de ameaça, o vigilante negará o acesso da pessoa suspeita ao recinto.

Seguindo essa linha, Kurose e Ross (2013) ressaltam que *firewall* é um equipamento que combina *hardware* e *software*, e que permite isolar uma rede interna de outra rede externa, permitindo e bloqueando determinados pacotes de dados.

De modo a controlar esse tráfego de dados, o *firewall* deve ser configurado com uma série de regras para filtrar todo o tráfego que ingressa ou sai de uma rede, de acordo com critérios estabelecidos. Dessa forma, o *firewall* converte-se em um importante componente na primeira linha de defesa de uma rede corporativa, aumentando consideravelmente a segurança dos dados que transitam no ambiente protegido.

2.4 PFSENSE

O *software* pfSense é uma distribuição FreeBSD, sistema operacional do tipo UNIX, de código aberto, e especificamente desenhada para utilização como *firewall*. Por muitos anos, o FreeBSD foi considerado o sistema operacional mais seguro do mundo (FreeBSD, 2021). O pfSense pode ser completamente administrado através de uma interface web e conta com recursos e características similares a maioria dos *firewalls* comerciais. Podemos citar como funcionalidades do pfSense: *Firewall*, NAT, Alta Disponibilidade, VPN, Servidor DNS, Servidor DHCP, entre outras.

Delfino (2020) ressalta que o pfSense é uma solução de *firewall* e/ou roteador muito robusta e amplamente utilizada, principalmente na intercomunicação das redes informáticas.

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, 2021).

3 METODOLOGIA

O presente estudo se desenrolará no formato de estudo de caso descritivo e exploratório, visando relacionar de forma não estatística os principais dados quantitativos a respeito da temática apresentada.

A investigação será do tipo descritiva, na medida em que serão analisadas e descritas as características e vantagens da utilização do *firewall* pfSense como solução de segurança na organização estudada, bem como expor suas fragilidades.

O campo de estudo será o Hotel Alojamento Local LTDA (nome da empresa é fictício), empresa que atua no ramo de hotelaria, com sede na região do Algarve, Portugal.

4 ANÁLISE DOS DADOS

4.1 HISTÓRICO DA ORGANIZAÇÃO ESTUDADA

O Hotel Alojamento Local LTDA (nome da empresa é fictício) é uma empresa que atua no ramo de hotelaria, com sede na região do Algarve, Portugal. Com a popularização da Internet, a unidade hoteleira foi compelida a criar uma estrutura para disponibilizar acesso à Internet aos seus hóspedes. Entretanto, suas políticas de

segurança de informação não conseguiram avançar na mesma velocidade do surgimento das novas tecnologias.

A empresa, objeto do presente estudo, conta com uma conexão de acesso à Internet por fibra ótica, contratada junto a um provedor local. A instalação dos equipamentos de comunicação (cabos, roteador, rede wifi, etc.) ficou a cargo do referido provedor, entretanto, observa-se que essa instalação, embora suficiente para estabelecer a comunicação com a Internet, não contempla uma solução robusta de *firewall*. O contexto apresentado resulta na existência de uma rede vulnerável aos ataques externos e com grande potencial para sofrer invasões informáticas.

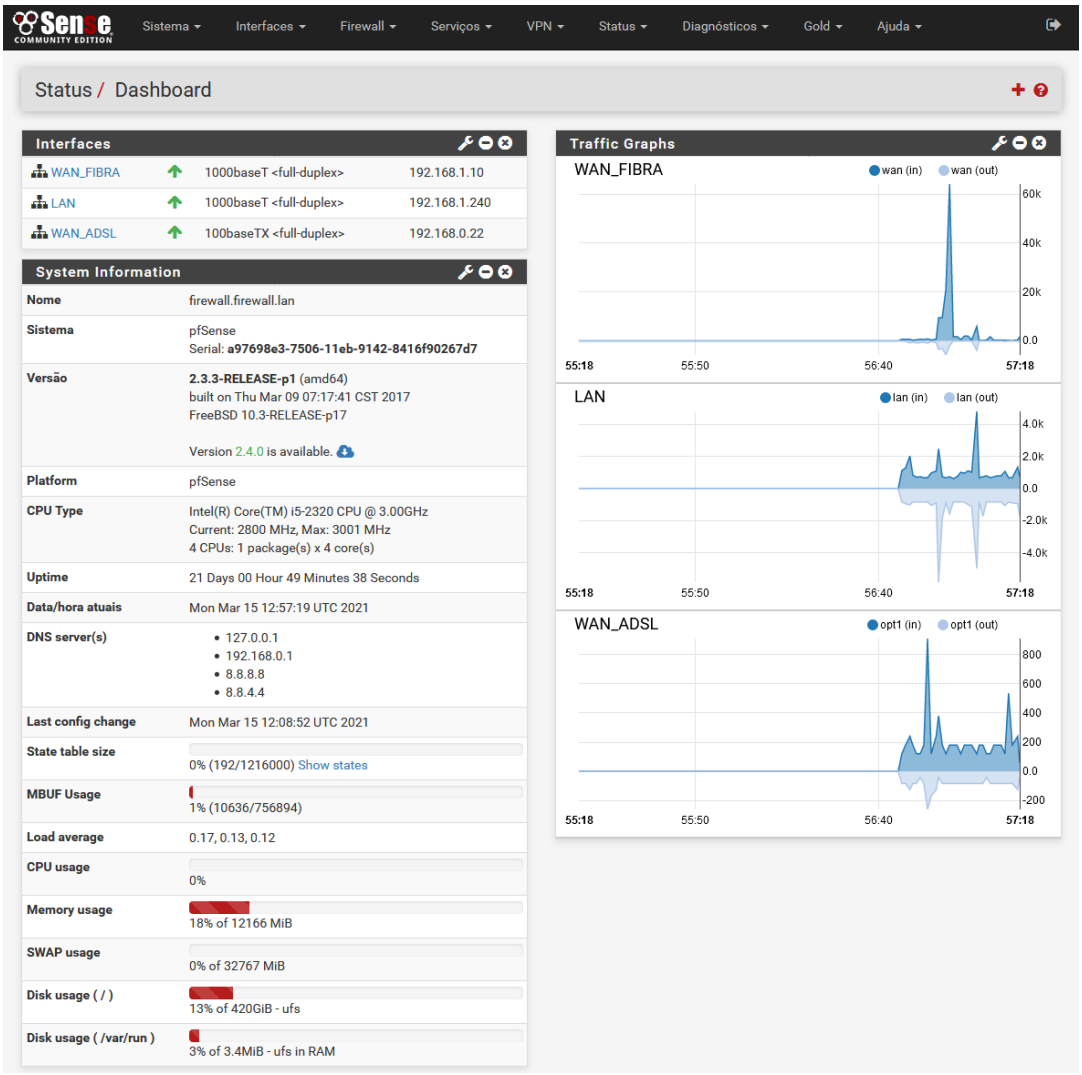
Em um contexto onde a empresa estudada utiliza as tecnologias da informação como parte integrante de seus processos, verifica-se a necessidade de contar com um sistema de segurança com o objetivo de proteger as informações que ingressam e saem da rede da empresa. Adicionalmente, a implantação de um *firewall* permitirá controlar os sites visitados, evitando que os usuários acessem conteúdos que não estejam de acordo com a política da organização e / ou possam colocar em risco a integridade da rede.

4.2 IMPLANTAÇÃO DO PFSENSE

Para restringir os riscos de ataques que possam afetar a empresa estudada, especialmente no que diz respeito aos riscos de invasão e roubo de informações confidenciais, o presente estudo propõe uma solução de segurança baseada na implantação de um *firewall* pfSense. O referido equipamento exercerá o controle sobre todos os dados que ingressam e saem da rede, atuando como uma barreira de proteção, salvaguardando a rede das ameaças externas.

A escolha pelo pfSense, em detrimento das demais opções disponíveis no mercado, deu-se pelo baixo custo associado ao projeto, a robustez, suas funcionalidades, bem como a capacidade de operar em equipamentos com características computacionais modestas, conforme pode-se observar na figura abaixo.

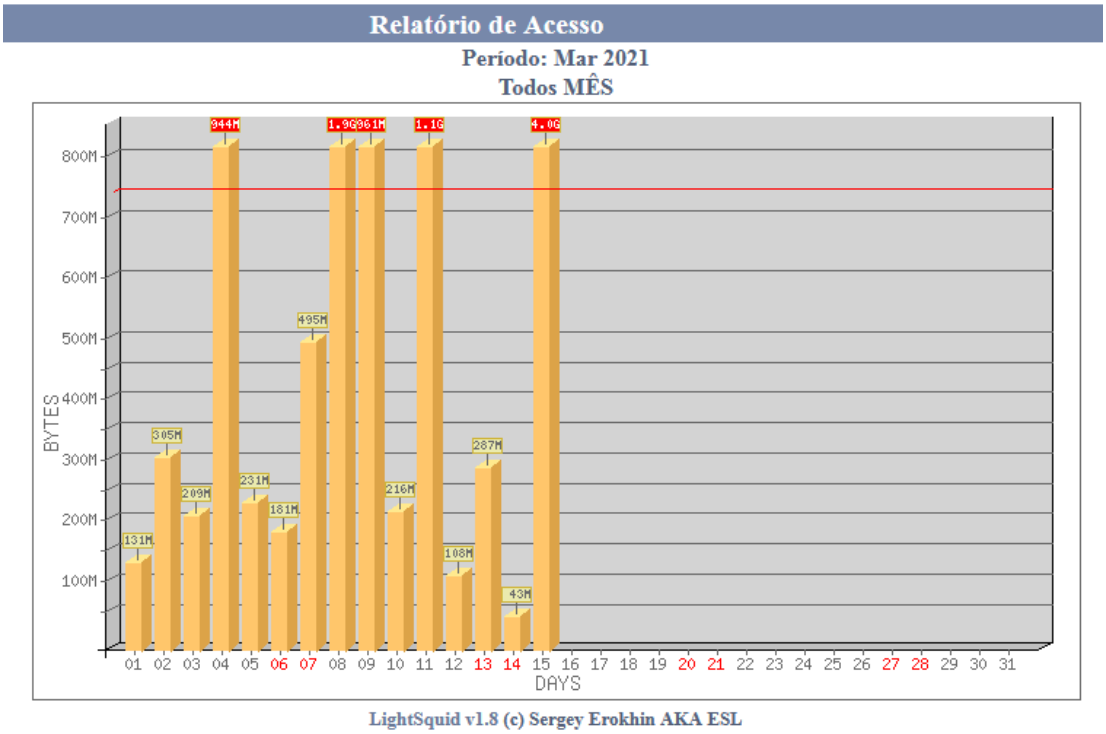
Figura 1 - Interface web de administração do pfSense.



Fonte: Captura de tela da empresa estudada (2021).

A solução proposta permite configurar um servidor *proxy* para aumentar a velocidade de acesso à Internet, através do uso de *cache*, além de filtrar milhares de sites que não estão de acordo com as políticas da organização, através da utilização de “listas negras” disponíveis (SquidGuard, 2021).

Figura 2 - Relatório de volume de tráfego diário na rede.



Fonte: Captura de tela da empresa estudada (2021).

Observa-se que a implantação de um servidor *firewall,* seguindo um critério bem estruturado de segurança da informação, permite resguardar a informação crítica e os processos internos da organização. Espera-se, portanto, não apenas mitigar os incidentes de segurança, mas também, possibilitar uma adequada gestão dos dados que transitam na rede corporativa.

4.3 SUGESTÕES DE MELHORIA

Novas ameaças e vulnerabilidades das redes informáticas surgem diariamente, exigindo que as organizações atualizem periódicamente suas políticas de segurança de informação.

Nesse sentido, sugere-se uma atitude pró-ativa nos temas relacionados com a segurança da rede informática. Os profissionais responsáveis devem definir políticas e normas de segurança, e garantir que os demais colaboradores tomem ciência das mesmas. Adicionalmente, sugere-se uma preocupação maior com o treinamento dos colaboradores em matéria pertinente ao assunto.

Como o *firewall* pfSense pode ser instalado em computadores com configurações modestas, devido ao fato de consumir poucos recursos de *hardware* (memória RAM, espaço em disco e processador), recomenda-se estudos complementares para observar a viabilidade de sua utilização em equipamentos com recursos limitados, tais como, *Raspberry Pi* ou similares.

5 CONSIDERAÇÕES FINAIS

Considera-se relevante a implantação de um *firewall* pfSense como solução de segurança para monitorar e controlar todos os dados que ingressam e saem da rede informática da empresa estudada. A referida solução busca manter a integridade da informação que transita pela rede, protegendo de ataques informáticos oriundos do exterior.

No caso estudado, foi possível monitorar e registrar a utilização da rede wifi, por parte dos hóspedes, bloqueando sites que não estejam de acordo com a política de segurança da organização, ou que sejam classificados como ameaças em potencial. Foi possível, graças a implantação da solução proposta, verificar que foram detectadas inúmeras tentativas de invasão ou acessos não autorizados, que em nenhum momento chegaram a afetar a normalidade do funcionamento da rede em questão.

Desse modo, o estudo respondeu afirmativamente a problemática investigativa que guiou o presente trabalho, ou seja, a solução de *firewall* pfSense mostrou-se apropriada em assegurar a funcionalidade da rede corporativa, facilitando a gestão dos processos de segurança, e protegendo-a de 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: 16 mar. 2021.

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. (13 de 11 de 2013). **Resources for Newbies**. Disponível em: < https://www.freebsd.org/projects/newbies/>. Acesso em: 16 mar. 2021.

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: 16 mar. 2021.

PFSENSE. **Getting Started**. Disponível em: < https://www.pfsense.org/getting-started/>. Acesso em: 16 mar. 2021.

SQUIDGUARD. **SquidGuard Blacklists**. Disponível em: < http://www.squidguard.org/blacklists.html>. Acesso em: 16 mar. 2021.

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: 16 mar. 2021.