A UTILIZAÇÃO DO *PFSENSE* COMO SOLUÇÃO PARA SEGURANÇA DE REDES

Danilo Duarte Antiquera[4]

Resumo. O presente trabalho tem como tema a utilização do *pfSense* como solução para segurança de redes. A metodologia adotada na formulação deste trabalho foi baseada em pesquisas bibliográficas, através de consultas a livros, revistas, pesquisa de manuais, tratados e artigos publicados na internet. O objetivo geral deste trabalho foi apresentar as principais vulnerabilidades a invasões e propor medidas para reforçar a segurança dos computadores. Tem-se como objetivo específico apresentar como instalar a ferramenta *pfSense* básica no ambiente virtual das organizações que utilizam essa forma de comunicação e conscientizar os usuários a utilizar a rede de forma mais produtiva e inteligente, fazendo com que a empresa se atualize em questão de segurança. Por fim, o presente trabalho deixa o tema em aberto propondo que no futuro se realize uma nova pesquisa bibliográfica seguida de um estudo de caso a fim de acrescentar outros recursos que o *pfSense* pode oferecer, transformando-se em uma ferramenta mais completa de segurança.

Palavras-chave: segurança em redes; *firewall*; *pfSense*.

Resumen. El uso de pfSense como solución para sguridad de redes. El presente trabajo tiene como tema el uso del pfSense como solución para Seguridad de Redes. La metodología adoptada en la formulación de este trabajo se basó en investigación bibliográfica, por medio de consultas con libros, periódicos, manuales, tratados, artículos publicados en internet. El objetivo general de este trabajo fue presentar las principales vulnerabilidades a las invasiones y proponer medidas para fortalecer la seguridad de las computadoras. Además, el objetivo también es presentar cómo instalar la herramienta básica pfSense en el ambiente virtual de las organizaciones, que utilizan esa forma de comunicación y concientizar a los usuarios sobre el uso de la red de manera más productiva e inteligente, haciendo que la empresa se actualice en seguridad. Por último, el presente trabajo deja el asunto en abierto proponiendo que en el futuro se realice una nueva investigación bibliográfica, seguida de un estudio de caso, a fin de agregar otros recursos que el pfSense pueda ofrecer en una herramienta más completa de seguridad.

Palabras clave: seguridad de redes; cortafuegos; pfSense.

Abstract. **The utilization of pfSense as a solution for network security.** The present work has as its theme the use of pfSense as a solution for Network Security. The methodology adopted in the formulation of this work has been based on bibliographical research through consultations with books, magazines, research of manuals, treaty, articles published on the internet. The general objective of this work was to present the main vulnerabilities to invasions and propose measures to enhance computer security. It has as its specific objective to also present how to install the basic pfSense tool in the virtual environment of organizations, which use this form of communication and to make users aware of using the network more productively and intelligently, causing the company to update itself on security issues. Finally, the present work leaves the subject open proposing that a new bibliographic research is to be done in the future followed by a case study in order to add other features that pfSense can offer and transforming it into a more complete security tool.

Keywords: network security; firewall; pfSense.

[4] Discente do Curso Superior de Gestão de Tecnologia da Informação da FATEC Itu. daniloduarteantiquera@gmail.com.

1 Introdução

Atualmente o homem precisa cada vez mais compartilhar recursos de forma rápida e objetiva para facilitar a comunicação com pessoas distantes. Em 1960, durante a Guerra Fria, foram criadas as redes de computadores para fins militares com o intuito de interconectar as bases e centros de comandos dos EUA para envio de dados. Os princípios de rede criados anos atrás ainda são usados para conectar as redes corporativas e estabelecer o compartilhamento de informações para os funcionários. Esses princípios se referem à interconexão por um sistema de comunicação baseado em transmissões e protocolos de comunicações de computadores, com o auxílio de outros recursos em paralelo, com o objetivo de compartilhar e ter acesso às informações em tempo real.

Com o aumento das organizações foi preciso facilitar a comunicação entre elas, introduzindo novas tecnologias. Diante disso, foi preciso interligar seus prédios ou empresas filiais por redes de computadores cabeadas ou sem fio, para compartilhar seus dados e informações e para agilizar as tarefas dos funcionários. No entanto, é preciso proteger essas informações e dados gerados pela empresa, bem como avaliar o grau de confiabilidade dos controles internos, a fim de assegurar sua adequação para se alcançar a missão institucional.

No ambiente corporativo é necessário orientar e conscientizar os usuários sobre possíveis falhas que podem estar ocorrendo e como a má utilização do sistema pode estar atrapalhando ao invés de ajudar a organização. Existem fatores externos tecnológicos que podem prejudicar a empresa, como possíveis ataques de *hackers* com ferramentas prontas e disponíveis na internet, que facilitam a intrusão, permitindo o vazamento de informações e roubos de projetos confidenciais.

O fator humano é uma brecha que faz relação com o fator externo, pois muitas vezes é o usuário que habilita ou facilita a entrada de invasores, por meio de um clique ou pela utilização de uma senha fraca. Assim, a segurança da informação é fortemente recomendada nas organizações para corrigir costumes e vícios dos usuários, através de monitoramento de programas instalados nos computadores para garantir ou minimizar as chances de alguém conseguir uma invasão. Para reforçar a segurança da rede corporativa, recomenda-se aplicar camadas de segurança com equipamentos sofisticados, uma política de segurança por escrito e devidamente assinada pelo Diretor e por todos os membros da corporação, além de atentar para as notícias do mundo tecnológico sobre falhas de segurança de *softwares*.

Nesta perspectiva, este artigo tem como foco propor medidas de enfrentamento dos problemas relacionados com a segurança do sistema, utilizando a ferramenta *pfSense*. As medidas de segurança aqui propostas poderão ser implementadas por qualquer empresa, todavia, serão soluções básicas que devem ser trabalhadas em conjunto para se tornarem

eficazes, observando que será necessário o comprometimento não só dos funcionários, mas principalmente da alta direção da organização apoiar o processo de segurança do sistema. Cabe salientar que a implementação de medidas de segurança de redes é um processo que exige atualizações constantes.

O objetivo geral deste trabalho é apresentar as principais vulnerabilidades a invasões e propor medidas para reforçar a segurança dos computadores e da rede, tal como a utilização da ferramenta *firewall pfSense*. Partindo do princípio de que os meios utilizados para se obter as informações das organizações e as técnicas utilizadas pelos invasores provocam perdas significativas de dados e informações, causando grandes impactos sobre as organizações e seus negócios, objetiva-se, também, apresentar uma maneira de aplicar uma camada de prevenção de invasões no ambiente virtual das organizações que utilizam essa forma de comunicação.

Como o firewall por si só não garante total segurança, é preciso conscientizar os usuários a utilizar a rede de forma mais produtiva e inteligente, fazendo com que a empresa sempre se atualize em questão de segurança. Nestes termos, este trabalho tem como objetivos específicos proporcionar uma visão estratégica para a organização sobre segurança em redes de computadores, mostrar a importância de se prevenir contra falhas de segurança nas redes corporativas e no armazenamento de dados e informações de forma seguram auxiliar os técnicos e profissionais em informática a implantar a ferramenta *pfSense* básica e conscientizar os usuários de que eles são um fator chave como alvos dos ataques.

A pesquisa é de fundamental importância para a evolução dos conhecimentos em determinado campo de estudo, ou seja, por meio da pesquisa pode-se ampliar os horizontes de conhecimento sobre determinado tema. A técnica adotada na formulação deste artigo foi a pesquisa bibliográfica, a partir da qual se fez uma leitura exploratória e analítica do material selecionado, tendo por finalidade ordená-lo e sumariar as informações pesquisadas e elaboradas. Neste processo, foi levado em consideração as informações que possibilitassem alcançar os objetivos gerais e específicos da pesquisa.

2 Segurança em redes

A segurança de rede consiste nas políticas e práticas adotadas para impedir e monitorar acesso não autorizado, uso indevido ou modificação de uma rede de computadores, contemplando os recursos por ela acessíveis. A segurança de rede envolve a autorização de acesso a dados, que é controlada pelo seu administrador. Os usuários escolhem ou recebem um ID e senha ou outras informações de autenticação que lhes permitem acesso a informações e programas dentro de sua autoridade. A segurança de rede abrange uma variedade de redes de

computadores públicas e privadas, que são usadas em tarefas cotidianas; condução de transações e comunicações entre empresas, agências governamentais e indivíduos. Ela protege a rede e protege e supervisiona as operações que estão sendo feitas.

A segurança da rede começa com a autenticação, geralmente com um nome de usuário e uma senha. Como isso requer um detalhe para autenticar o nome do usuário, a senha, é chamado de autenticação de um fator, podendo ser também a autenticação de dois fatores, algo que o usuário 'tem' também é usado (por exemplo, um token de segurança, um cartão de caixa eletrônico ou um telefone celular); ou autenticação de três fatores, algo em que o usuário também é usado (por exemplo, uma impressão digital ou escaneamento de retina). Uma vez autenticado, um firewall impõe políticas de acesso, como quais serviços podem ser acessados pelos usuários da rede. (CORRÊA, 2015)

Embora seja eficaz para impedir o acesso não autorizado, este componente pode falhar na verificação de conteúdo potencialmente nocivo, como *worms* de computador ou cavalos de Tróia, que são transmitidos pela rede. Um *software* antivírus ou um Sistema de Prevenção de Intrusão (IPS) ajuda a detectar e inibir a ação desse *malware* (SIMMONDS; SANDILANDS; VAN EKERT, 2004). Um sistema de detecção de intrusos baseado em anomalias também pode monitorar a rede, como o tráfego *wireshark*, registrando-o para fins de auditoria e posterior análise de alto nível. Os sistemas mais recentes, que combinam aprendizado de máquina sem supervisão com análise de tráfego de rede completa, podem detectar invasores de rede ativos de usuários internos mal-intencionados ou invasores externos direcionados que comprometeram uma máquina ou conta de usuário. (HUBBARD, 2008)

A comunicação entre dois *hosts* usando uma rede pode ser criptografada para manter a privacidade. Os *honeypots*, que basicamente atraem recursos acessíveis pela rede, podem ser implantados como ferramentas de vigilância e de alerta antecipado, pois normalmente não são acessados para fins legítimos. Técnicas utilizadas pelos atacantes que tentam comprometer esses recursos de chamariz são estudadas durante e após um ataque para manter um olho em nova exploração técnica. Essa análise pode ser usada para aumentar ainda mais a segurança da rede real que está sendo protegida; ou seja, direcionar a atenção de um invasor para longe de servidores legítimos, encorajando-o a gastar seu tempo e energia no servidor *decoy* enquanto distraem sua atenção dos dados no servidor real.

> Semelhante a um honeypot, uma honeynet é uma rede configurada com vulnerabilidades intencionais. Sua finalidade também é convidar ataques para que os métodos do invasor possam ser estudados e que as informações possam ser usadas para aumentar a segurança da rede. Uma honeynet normalmente contém um ou mais honeypots. (NAKAMURA, 2010, p. 276)

3 Política de segurança de rede

Política de segurança é uma definição do que significa ser seguro para um sistema, organização ou outra entidade. Para uma organização, ela aborda as limitações de comportamento de seus membros, bem como as restrições impostas aos adversários por mecanismos como portas, fechaduras, chaves e muros. Para um sistema, a política de segurança aborda as restrições de funções e fluxo entre elas, restrições de acesso por sistemas externos e adversários, incluindo programas e acesso a dados por pessoas.

Se for importante ser seguro, é preciso ter certeza de que toda a política de segurança é imposta por mecanismos suficientemente fortes. Existem muitas metodologias organizadas e estratégias de avaliação de risco para garantir a integridade das políticas de segurança e assegurar que elas sejam completamente aplicadas. Em sistemas de informações, as políticas podem ser decompostas em subpolíticas para facilitar a alocação de mecanismos de segurança para impor subpolíticas.

Não obstante, esta prática tem armadilhas. É muito fácil simplesmente ir diretamente para as subpolíticas, que são essencialmente as regras de operação, e dispensar a política de nível superior. Isso dá a falsa impressão de que as regras de operação abordam alguma definição geral de segurança. Por ser difícil pensar com clareza quanto à integridade em relação à segurança, as regras de operação declaradas como "subpolíticas" sem nenhuma "superpolítica" geralmente se transformam em regras incoerentes que não reforçam nada com perfeição. Consequentemente, uma política de segurança de nível superior é essencial para qualquer esquema de segurança sério e as subpolíticas e regras de operação não têm sentido sem ela.

Uma política de segurança de rede, ou NSP, é um documento genérico que delineia regras para o acesso à rede de computadores, determina como as políticas são aplicadas e estabelece algumas das arquiteturas básicas do ambiente de segurança de rede/segurança da empresa. O documento em si é geralmente de várias páginas e escrito por um comitê. Uma política de segurança vai muito além da simples ideia de "manter os bandidos de fora". É um documento muito complexo, destinado a reger o acesso aos dados, uso de senhas e criptografia, e-mails, anexos e muito mais. Ele específica as regras para indivíduos ou grupos de indivíduos em toda a empresa.

A política de segurança deve exercer controle sobre os usuários mal-intencionados e aqueles com potencial de risco para a organização. O primeiro passo na criação de uma política é entender quais informações e serviços estão disponíveis (e para quais usuários), qual é o potencial para danos e se já existe alguma proteção para evitar o uso indevido. Além disso, a política de segurança deve ditar uma hierarquia de permissões de acesso; isto é, conceder aos usuários acesso apenas ao que é necessário para a conclusão de seu trabalho.

Enquanto escrever o documento de segurança pode ser um grande empreendimento, um bom começo pode ser alcançado usando um modelo. O Instituto Nacional de Padrões e Tecnologia fornece uma diretriz de política de segurança. As políticas podem ser expressas como um conjunto de instruções que podem ser compreendidas pelo *hardware* de rede para fins especiais de proteção à rede.

3.1 *Firewall*

Na computação, um *firewall* é um sistema de segurança de rede que monitora e controla o tráfego de entrada e saída da rede com base em regras de segurança predeterminadas. Segundo Correa (2015), geralmente ele estabelece uma barreira entre uma rede interna confiável e uma rede externa não confiável, como a Internet. De acordo com Hubbard (2008), o termo *firewall* originalmente se referia a uma parede destinada a confinar um incêndio dentro de um edifício, mas usos posteriores referem-se a estruturas semelhantes, como a folha de metal que separa o compartimento do motor de um veículo ou aeronave do compartimento de passageiros. À tecnologia de rede, o termo foi aplicado no final dos anos 1980, quando a Internet era relativamente nova em termos de uso e conectividade global, sendo que, conforme descreve Miller (2008), os predecessores de *firewalls* para segurança de rede foram os roteadores usados no final dos anos 1980.

Os *firewalls* geralmente são categorizados como baseados em rede ou em *host*. Os *firewalls* baseados em rede estão posicionados nos computadores de *gateway* das LANs, WANs e intranets. Eles são dispositivos de *software* em execução em *hardware* de finalidade geral ou dispositivos de computador de *firewall* baseados em *hardware*. Os dispositivos de *firewall* também podem oferecer outras funcionalidades à rede interna que protegem, como atuar como um servidor DHCP ou VPN para essa rede. Os *firewalls* baseados em *host* são posicionados no nó da rede e monitoram o tráfego de rede dentro e fora dessas máquinas, podendo ser um *daemon* ou serviço, como parte do sistema operacional ou de um aplicativo de agente, como segurança ou proteção de *endpoint*. Cada um tem vantagens e desvantagens, mas também um papel na segurança em camadas. Os *firewalls* também variam em tipo dependendo de onde a comunicação é originada, onde é interceptada e do estado da comunicação a ser rastreada. (STALLINGS, 2008)

Os *firewalls* de camada de rede, também chamados de filtros de pacotes, operam em um nível relativamente baixo da pilha de protocolos TCP/IP, não permitindo que os pacotes passem pelo *firewall*, a menos que correspondam ao conjunto de regras estabelecido. O administrador do *firewall* pode definir as regras; ou regras-padrão podem ser aplicadas. Os *firewalls* da

camada de rede geralmente se enquadram em duas subcategorias, com estado e sem estado. Os filtros de pacotes[5] comumente usados em várias versões do Unix são ipfw (FreeBSD, Mac OS X (10.7)), NPF (NetBSD), PF (Mac OS X (> 10.4), OpenBSD e alguns outros BSDs), iptables/ipchains (Linux) e IPFilter.

Os *firewalls* da camada de aplicativo funcionam no nível de aplicativo da pilha TCP / IP (ou seja, todo o tráfego do navegador ou todo o tráfego telnet ou FTP), e podem interceptar todos os pacotes que viajam para ou que vêm de um aplicativo, determinando se um processo deve aceitar qualquer conexão. Os *firewalls* de aplicativos realizam suas funções conectando-se a chamadas de soquete[6] para filtrar as conexões entre a camada de aplicativo e as camadas inferiores do modelo OSI. Os *firewalls* de aplicativos funcionam como um filtro de pacotes, mas os filtros de aplicativos aplicam regras de filtragem (permissão/bloqueio) por processo, em vez de filtrar conexões por porta. Geralmente, os *prompts* são usados para definir regras para processos que ainda não receberam uma conexão, sendo raro encontrar *firewalls* de aplicativos não combinados ou usados em conjunto com um filtro de pacotes.

Além disso, os *firewalls* de aplicativos filtram ainda mais as conexões examinando o ID do processo dos pacotes de dados em relação a um conjunto de regras para o processo local envolvido na transmissão de dados. A extensão da filtragem que ocorre é definida pelo conjunto de regras fornecido. Dada a variedade de softwares existentes, os *firewalls* de aplicativos só têm conjuntos de regras mais complexos para os serviços padrão, como serviços de compartilhamento. Esses conjuntos de regras por processo têm eficácia limitada na filtragem de todas as associações possíveis que podem ocorrer com outros processos. Além de tudo, esses conjuntos de regras por processo não podem se defender contra a modificação do processo por meio de exploração, como falhas de corrupção de memória. Devido a essas limitações, os *firewalls* de aplicativos estão começando a ser substituídos por uma nova geração que dependem do controle de acesso obrigatório, o MAC, também conhecido como *sandboxing*. (BRUGESS, 2006)

Um servidor *proxy* (executado em *hardware* dedicado ou como *software* em uma máquina de propósito geral) pode atuar como um *firewall* respondendo a pacotes de entrada (solicitações de conexão, por exemplo) da maneira de um aplicativo, enquanto bloqueia outros pacotes. Um servidor *proxy* é um *gateway* de uma rede para outra para um aplicativo de rede específico, no sentido de que ele funciona como um *proxy* em nome do usuário da rede. (SIMMONDS; SANDILANDS; VAN EKERT, 2004)

[5] O termo "filtro de pacotes" originou-se no contexto dos sistemas operacionais BSD.
[6] *Firewalls* de aplicativos que se conectam a chamadas de soquete também são chamados de filtros de soquete.

Proxies dificultam a adulteração de um sistema interno da rede externa, de modo que o uso indevido de um sistema interno não causa necessariamente uma violação de segurança explorável fora do *firewall* (desde que o *proxy* do aplicativo permaneça intacto e configurado adequadamente). Por outro lado, intrusos podem sequestrar um sistema acessível ao público e usá-lo como um *proxy* para seus próprios propósitos; o *proxy* então se disfarça desse sistema para outras máquinas internas. Embora o uso de espaços de endereço internos aumente a segurança, os *crackers* ainda podem empregar métodos como *spoofing* de IP para tentar passar pacotes para uma rede de destino.

3.2 *pfSense*

O *pfSense* é uma distribuição de *software* de computador de *firewall* / roteador de código aberto baseada no FreeBSD[7] e adaptado para assumir o papel de um *firewall* e/ou roteador de redes. Ele possui recursos que muitas vezes são encontrados apenas em *firewalls* comerciais caros, já que é possível realizar com o *pfSense* a imensa maioria das atividades esperadas por sistemas com esse título. (CORRÊA, 2015)

> O projeto pfSense foi concebido em meados de setembro de 2004 por Chris Buechler e Scott Ullrich. Chris foi um colaborador assíduo de códigos por muito tempo do projeto m0n0wall[8]. O m0n0wall tem basicamente as mesmas pretensões técnicas do pfSense, mas desde o seu surgimento até o fim de seu desenvolvimento, seu foco foi em appliances. (HUBBARD, 2008)

Como apresentado anteriormente, um *firewall* funciona como uma barreira (ou "escudo") entre o computador e o ciberespaço. O *pfSense* é um *software* de *firewall* altamente versátil. Por possuir pacotes adicionais o transformando-se em um UTM (“Gerenciamento Unificado de Ameaças”). É composto de diversos serviços como VPN, balanceamento de carga, regras de NAT, regras de *Firewall*, geração de chaves RSA e monitoramento de tráfego. Está rapidamente se tornando a solução de segurança de rede de código aberto mais confiável do mundo. Possui uma gama de *softwares* gratuitos para funcionalidades de monitoramento dentro de uma rede como Snort, IDS, IPS, NIDS. O *Snort* é uma ferramenta NIDS *open-source* desenvolvida por Martin Roesch sendo muito popular pela sua flexibilidade nas configurações de regras e constante atualização diante das ferramentas de invasão de licença livre. Seu código fonte otimizado, é desenvolvido em módulos utilizando a linguagem C possuindo documentação de domínio público. (BRUGESS, 2006).

[7] O *FreeBSD* fornece compatibilidade binária com muitas outras variações do Unix e também é compatível com o sistema operativo GNU/Linux.
[8] O *m0n0wall* tem basicamente as mesmas pretensões técnicas do *pfSense*, mas desde o seu surgimento é focado em *appliances*, ou seja, equipamentos específicos para desempenhar uma determinada função.

O *Intrusion Detection System* (IDS) é um **s**istema de detecção de intrusão em rede que pode atuar de dois modos distintos: na rota dos pacotes, no qual captura e analisa os pacotes e depois os encaminha para o próximo salto de sua rota; e fora da rota, no qual os pacotes são espelhados em um comutador, sendo encaminhados tanto para um Sistema de Detecção de Intrusão, quanto para o seu próximo destino na rota. (MORAES, 2010).

Os IPS online são capazes de finalizar as conexões enviando mensagens do tipo "*drop*" antes que cheguem ao destino, como acontece nas atividades de um *firewall*, diferentemente do que acontece nos IPS com operação em modo passivo, onde possuem formas de atuação normalmente com o envio de mensagens "TCP reset", possibilitando ao atacante obter informações que podem ser relevantes aos ataques. (KENNEDY, 2016).

O *Network-Based Intrusion Detection System* (NIDS), por sua vez, é um sistema de detecção de intrusos baseado em rede que monitora a atividade do tráfego em um determinado segmento de rede, utilizando normalmente suas interfaces de rede em modo promíscuo. A detecção é feita com a captura dos pacotes e análise comparativa com padrões ou assinaturas conhecidas pelo NIDS. (KENNEDY, 2016)

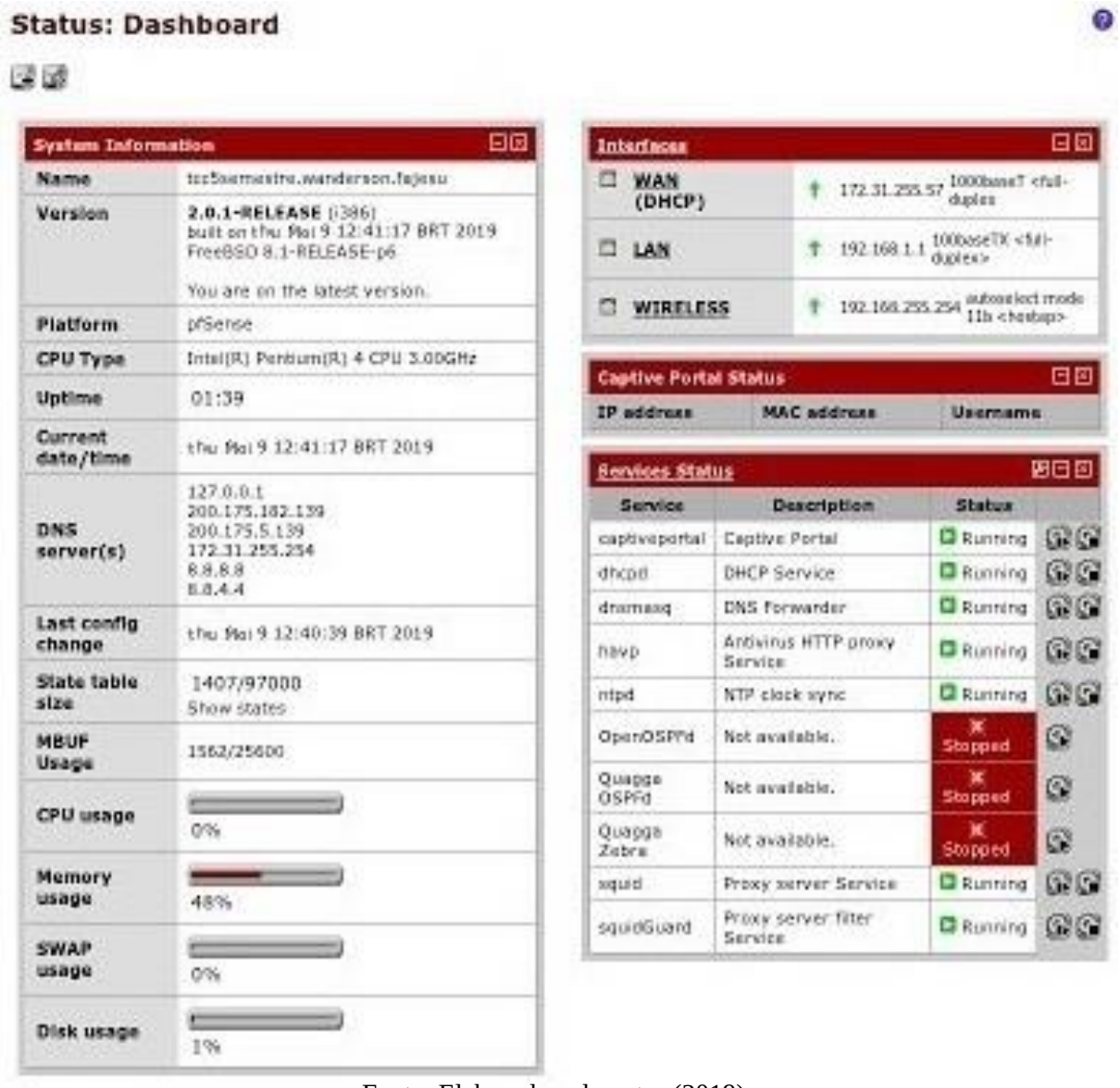
Apesar do *pfSense* ser um *Unix* não é necessário que o usuário seja *expert* nesta modalidade de sistema. Por ser um sistema pré-programado, ele se parece como uma instalação do Linux, bastando apenas que, após a instalação, sejam adicionadas as configurações necessárias, utilizando um navegador web. Todavia, o utilizador deve possuir conhecimentos em protocolos e segurança de rede para configurá-lo corretamente.

Figura 1 – Tela inicial do *pfSense*

Fonte: Elaborado pelo autor (2019).

A instalação só exige que o computador tenha pelo menos duas placas de rede, para que se tenha a Wan (internet) e a Lan (rede interna), conforme mostra a Figura 1. A referida figura ilustra a tela inicial do *pfSense* em modo texto(cmd), onde já foi feita a instalação no *hardware* e mostra as opções que se pode acessar em modo texto. Pode ser também acessada remotamente pelo IP da Lan, a tela inicial em *dashboard*, conforme mostra a Figura 2.

Figura 2 – Tela inicial do *pfSense (dashboard)*



Fonte: Elaborado pelo autor (2019).

As regras ficam no menu firewall como mostra a Figura 3. Nesse menu constam regras de entrada da Wan e da Lan. São 3 regras bem básicas, mas que fazem total sentido quando se pensa em fazer uma segurança básica. Com essas 3 regras faz-se com que sejam passadas todas as solicitações por dentro do *pfSense*. E não haverá problemas com relação a controles de acesso, porque tudo vai estar controlado pelo *pfSense*.

Figura 3 – Regras de *firewall*

Fonte: Elaborado pelo autor (2019).

Como ilustra a Figura 4, a primeira ação é “passar”, mas tem também “bloquear” ou “rejeitar”. A primeira (padrão) deixa passar tudo, ou seja, está tudo liberado. Pode-se deixar passar apenas alguns protocolos. Então marca-se a opção Pass. Na interface mantem-se LAN, em TCP/IP mantem-se o IPv4, e em protocolo escolhe-se UDP, somente no exemplo acima em que se coloca a porta de destino 53 que é de DNS. Tem-se também como marcar a origem e destino. Na origem, pode-se dizer que é a LAN Net e no destino pode-se colocar qualquer um. Agora precisa-se liberar mais 2 portas para a internet funcionar: a porta 80, que é a HTTP, e a porta 443, que é a HTTPS. Feito isso, tem-se um *firewall* bem funcional.

Figura 4 – Portas adicionadas

Fonte: Elaborado pelo autor (2019).

4 Considerações finais

O presente trabalho teve como tema a utilização do *pfSense* como solução para segurança de redes, considerada viável por ser gratuita e com amplas ferramentas adicionais. A metodologia adotada foi baseada em pesquisas bibliográficas e o objetivo geral foi apresentar as principais vulnerabilidades a invasões, propondo a implantação da ferramenta *firewall pfSense* básica para reforçar a segurança da rede.

Foi possível perceber a importância do *pfSense*. Sua criação em todas as funcionalidades existentes no m0n0wall, com melhorias de interface web de configuração e uma aproximação com as versões recentes do *FreeBSD* (sistema base), conquistou usuários pelo fato de ser extremamente organizado e agregar uma série de outras funcionalidades com fácil acesso, o que permite a quem tenha conhecimentos básicos de redes instalá-lo e gerenciá-lo.

O *firewall* por si não garante total segurança, de modo que é preciso conscientizar os usuários a utilizarem a rede de forma produtiva e inteligente, do mesmo modo que a empresa de se atualizar em questão de segurança. O tema fica em aberto, carente de uma nova pesquisa, a fim de acrescentar outros recursos que o *pfSense* pode oferecer.

5 Referências

BRUGESS, M. Princípios de Administração de Redes e Sistemas. 2. ed. Rio de Janeiro: LTC, 2006.

CORRÊA, M. P. *PfSense: O Guia Ideal para Iniciantes*. Tubarão/SC: Elelux, 2015.

HUBBARD, J. A *Role-Based Trusted Network Provides Pervasive Security and Compliance* - interview with Jayshree Ullal, senior VP of Cisco (January 02, 2008). Disponível em: <https://newsroom.cisco.com/feature-content?type=webcontent&articleId=4124873> Acesso em: 22 nov. 2018.

KENNEDY, P. *pfSense adopts apache 2.0 License*. STH FORUM (2016). Disponível em: https://www.servethehome.com/pfsense-adopts-apache-2-0-license/. Acesso em: 18 out. 2018.

MILLER, S. *Configure a professional firewall using pfSense*. (26 jun. 2008). Disponível em <http://freesoftwaremagazine.com/articles/configure_professional_firewall_using_pfsense/> Acesso em: 18 out. 2018.

MORAES, A. F. de. *Fundamentos de Segurança em Redes***.** São Paulo: Érica, 2010.

NAKAMURA, E. T.; GEUS, P. L. de. *Segurança de Redes em Ambientes Cooperativos***.** São Paulo: Novatec, 2010.

SIMMONDS, A; SANDILANDS, P; VAN EKERT, L An Ontology for Network Security Attack. *Lecture Notes in Computer Science*, v. 3285, p. 317–323, 2004. Disponível em: <http://www.sciepub.com/reference/103339>. Acesso em: 18 out. 2018.

STALLINGS, W. *Criptografia e segurança de redes***.** São Paulo: Pearson, 2008.