MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TOCANTINS *CAMPUS* DIANÓPOLIS
CURSO DE LICENCIATURA EM COMPUTAÇÃO

PEDRO HENRIQUE RIBEIRO DE AGUIAR

ESTUDO DE CASO: Implementação de NGFW na rede corporativa Escola Estadual Coronel Abílio Wolney

DIANÓPOLIS
2023

PEDRO HENRIQUE RIBEIRO DE AGUIAR

ESTUDO DE CASO: Implementação de NGFW na rede corporativa Escola Estadual Coronel Abílio Wolney

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Computação do *Campus* Dianópolis Instituto Federal de Educação, Ciência e Tecnologia do Tocantins, como exigência à obtenção do título de licenciado em Computação.

Orientador: Dr. Lucas Arruda Ramalho

DIANÓPOLIS
2023

Dados Internacionais de Catalogação na Publicação (CIP)
Bibliotecas do Instituto Federal do Tocantins

A283e Aguiar, Pedro Henrique Ribeiro de
ESTUDO DE CASO: Implementação de NGFW na rede corporativa Escola Estadual Coronel Abílio Wolney / Pedro Henrique Ribeiro de Aguiar. – Dianópolis, TO, 2023.
34 f. : il. color.

Trabalho de Conclusão de Curso (Licenciatura em Computação) – Instituto Federal de Educação, Ciência e Tecnologia do Tocantins, Campus Dianópolis, Dianópolis, TO, 2023.

Orientador: Dr. Lucas Arruda Ramalho

1. Firewall. 2. Segurança. 3. Inovações Tecnológicas. I. Ramalho, Lucas Arruda. II. Título.

CDD 004

A reprodução total ou parcial, de qualquer forma ou por qualquer meio, deste documento é autorizada para fins de estudo e pesquisa, desde que citada a fonte.

Elaborado pelo sistema de geração automatica de ficha catalográfica do IFTO com os dados fornecidos pelo(a) autor(a).

PEDRO HENRIQUE RIBEIRO DE AGUIAR

ESTUDO DE CASO: Implementação de NGFW na rede corporativa Escola Estadual Coronel Abílio Wolney

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Computação do *Campus* Dianópolis Instituto Federal de Educação, Ciência e Tecnologia do Tocantins, como exigência à obtenção do título de licenciado em Computação.

Aprovado em: 06/12/2023

BANCA AVALIADORA

_____

Prof. Dr. Lucas Arruda Ramalho
IFTO – *Campus Dianópolis*

_____

Prof. Valber Sardi Lopes
IFTO – *Campus Dianópolis*

_____

Prof. Theylor Sousa Santos
Externo

DIANÓPOLIS-TO

2023

EPÍGRAFE

“O mundo é grande, então basta sonhar, eu tô na luta pra ser campeão, Deus me deu asas pra voar, mas sem tirar os pés do chão.”

Lipi (2023)

“Vou sonhar mesmo, também posso conquistar.”

Cebezinho (2023)

AGRADECIMENTOS

Agradeço primeiramente a Deus que sempre me deu forças para continuar, e aos meus pais: Ernesto e Maria Helena, que são minha maior inspiração e nunca mediram esforços para fazerem de tudo pela nossa família, pretendo honrá-los muito ainda. Tenho total gratidão a minha família que sempre me apoiou e sempre admiraram minha garra e foco. Tenho prazer em agradecer meus amigos por todo o incentivo, os momentos e histórias que teremos para contar, vocês são incríveis e sabem disso. E não pode faltar minha eterna gratidão ao meu orientador Dr. Lucas Ramalho, que deu total apoio e pôs o braço para que eu fizesse desse trabalho um grande mar de conhecimento e experiência para toda a vida. Sou grato por todos que fizeram e fazem parte da minha vida acadêmica e pessoal, tenho certeza que todo esse esforço valeu a pena para um grande sucesso.

Também sou grato a mim por sempre manter os pés no chão e nunca desistir dos meus sonhos e objetivos, mesmo nos momentos mais difíceis, tive fé e um foco que nunca deve ser deixado para trás. Mãe e Pai, isso é por vocês, amo os senhores infinitamente S2. Eu ainda vou dominar esse mundo, Fé em Deus que Ele é justo.

RESUMO

Com o avanço das tecnologias e das maneiras de acessar sites, e também com a evolução dos tipos de ataques, um firewall tradicional já não é suficiente para proteger adequadamente um ambiente corporativo. Para se manter atualizado com essas mudanças, é necessário usar um NGFW, ou seja, um Firewall de Nova Geração. Neste trabalho, será falado sobre o Firewall Pfsense e o Mikrotik Routerboard 750 Gr3 que fazem parte dessa constante evolução e são bem acessíveis. Também vamos discutir os princípios da segurança da informação e alguns conceitos importantes que fazem parte de toda a gama de redes e sua segurança: como vulnerabilidades, riscos, ataques, precauções a serem tomadas e as principais regras de *firewall* usadas na construção do trabalho.

Para o desenvolvimento do trabalho, foram utilizados os conceitos de redundância, failover, load balance e regras de firewall. Uma parte do projeto foi implementado no VirtualBox, no caso do PfSense e a outra parte foi prática, onde foi utilizado o Mikrotik. Concluiu-se que as duas soluções obtiveram resultados bem parecidos.

Por fim, nosso objetivo principal é mostrar as inovações tecnológicas de um NGFW(Firewall de Nova Geração) e como o software foi útil para toda a construção do trabalho. É importante lembrar também que nenhum ambiente é totalmente seguro, já que as ameaças e as soluções estão em constante evolução. Portanto, é importante entender as necessidades do ambiente para encontrar a melhor solução, considerando as diversas opções disponíveis no mercado, cada uma com suas próprias características.

Palavras-chave: Firewall tradicional, inovações tecnológicas, NGFW, Segurança.

ABSTRACT

With the advancement of technologies and ways to access websites, along with the evolution of attack types, a traditional firewall is no longer sufficient to adequately protect a corporate environment. To stay updated with these changes, it is necessary to use a Next-Generation Firewall (NGFW). In this paper, we will discuss the Pfsense Firewall and the Mikrotik Routerboard 750 Gr3, which are part of this constant evolution and are quite accessible. We will also delve into the principles of information security and some important concepts that are integral to the entire realm of networks and their security, such as vulnerabilities, risks, attacks, precautions to be taken, and the main firewall rules used in the construction of the work.

For the development of the project, concepts of redundancy, failover, load balancing, and firewall rules were employed. A portion of the project was implemented in VirtualBox, in the case of PfSense, and the other part was practical, involving the use of Mikrotik. It was concluded that both solutions yielded very similar results.

In conclusion, our main objective is to showcase the technological innovations of an NGFW (Next-Generation Firewall) and how the software was instrumental in the entire construction of the project. It is important to note that no environment is entirely secure, as threats and solutions are in constant evolution. Therefore, understanding the needs of the environment to find the best solution is crucial, considering the various options available in the market, each with its own characteristics.

Keywords: NGFW (Next-Generation Firewall), Security, Traditional firewall, technological innovations.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

DHCP - Dynamic Host Configuration Protocol

DNS - Sistema de Nomes de Domínio

IPsec - Protocolo de Segurança

LAN - Rede de Área Local

NGFW - Firewall de Nova Geração

OpenVPN - Protocolo de VPN de código aberto

PC - Computador Desktop

PPTP - Protocolo de Tunelamento Ponto-a-Ponto

Vlan - Virtual Area Local Network

VM - Máquina virtual

VPN - Virtual Private Network

SUMÁRIO

1 INTRODUÇÃO

A rede de computadores é fundamental para a comunicação e compartilhamento de informações e para (Tanenbaum, 1996) uma rede de computadores é uma coleção de computadores autônomos interconectados por uma única tecnologia. As redes são compostas por dispositivos eletrônicos como: servidores, dispositivos de rede, computadores e entre outros. Eles estão interligados para fornecer um sistema que facilita o compartilhamento de recursos e a comunicação. São ferramentas indispensáveis para a comunicação moderna, pois permitem o acesso à informação, a colaboração de pessoas e o compartilhamento de dados e recursos. Isso os torna uma parte fundamental de nossas atividades diárias.

Mas em meio a toda essa evolução tecnológica, a segurança é um aspecto essencial em redes de computadores e deve ser tratada com grande importância, pois é fundamental nas redes corporativas e demais empresas que partilham bastante informações diárias (Kurose, 2009). É baseado nesse pensamento que ferramentas como os firewalls são amplamente utilizados e estão em crescente atualização.

Os firewalls trabalham examinando os pacotes de dados que atravessam a rede e aplicam políticas de segurança para determinar se um pacote deve ser permitido ou bloqueado. As políticas podem ser baseadas em endereços IP, portas de comunicação, protocolos, serviços e outros critérios.

Sabendo que não existem sistemas 100% seguros, essas barreiras de segurança são capazes de fazer a proteção da rede e possibilitam ao administrador da rede configurar as políticas de segurança que sua rede necessita. Com o passar dos anos, a evolução das aplicações e juntamente com a evolução dos ataques, firewalls tradicionais não são mais suficientes para proteger com eficácia ambientes corporativos. Por isso, surge o conceito dos Firewalls de Nova Geração (NGFW).

Levando em consideração os aspectos dos "firewalls ", foi implementado um projeto na Escola Estadual Coronel Abílio Wolney que teve como objetivo a melhoria da rede e o gerenciamento com a utilização dessa barreira de segurança/parede de fogo, que se trata do Firewalls de Nova Geração. Esses firewalls são divididos em dois tipos: Firewall de Hardware e Software. Os de hardware, são os aparelhos físicos que são criados apenas para controlar o tráfego e melhorar o gerenciamento e segurança da rede,eles ficam entre a rede externa e a rede local como no caso do mikrotik RB 750 Gr 3 que foi implementado na rede corporativa escolar.

Já os firewalls de software são os sistemas alocados por meio de downloads para um desktop ou notebook de utilização, sua implementação é crucial, pois é essa camada que faz com

que o usuário final possa enviar e receber pacotes com mais segurança. A aplicação do Firewall de software que foi utilizado é o PfSense, sua aplicação destinou-se a ser feita em uma VM para possíveis testes.

Neste presente trabalho foram usados como análise o PfSense e o equipamento Mikrotik RB(Routerboard 750 Gr 3), que trazem novidades e funções de segurança complementares aos firewalls tradicionais, que são elas: Inspeção profunda de pacotes, detecção de ameaças avançadas, filtragem de aplicativos, prevenção de intrusões e muito mais.

O objetivo deste trabalho é analisar o potencial das ferramentas e como sua utilização é necessária para segurança no gerenciamento de redes corporativas e prevenção de incidentes de segurança. Para isso, será realizado um tutorial básico de instalação e configuração das principais funções de segurança para esses ambientes.

Este trabalho está organizado em capítulos. No Capítulo 1 está a introdução do trabalho, onde é explicado brevemente sobre o tema escolhido e o objetivo da pesquisa . No Capítulo 2 será inserido o embasamento teórico necessário ao entendimento dos principais conceitos abordados no trabalho e em sequência, tópicos que favorecem o entendimento do trabalho . No Capítulo 3 está localizada a metodologia da pesquisa, que fala sobre os conceitos, métodos e técnicas que contribuíram para o desenvolvimento e a descrição do trabalho. No Capítulo 4 a pesquisa de campo, que apresentará os resultados e análises. No Capítulo 5 se encontram as considerações finais, onde ficaram as principais descobertas e o resultado dessa pesquisa. E por fim, no Capítulo 6 se encontram as referências bibliográficas utilizadas para a conclusão do trabalho.

2 EMBASAMENTO TEÓRICO

Neste item serão abordados alguns dos principais conceitos do tema do presente trabalho, como: Modelo OSI, Vlan, Firewall e subtópicos sobre regras de segurança, Nat, Balanceamento e demais configurações, tanto do PfSense como do aparelho Mikrotik RB.

2.1 Modelo OSI

O modelo de referência OSI (Open System Interconnection) é um estrutura de protocolos que permite a comunicação entre diferentes sistemas. A estrutura dos sistemas em comunicação deve seguir a referência de 7 camadas, como ilustrado na Figura 1, definidas no modelo OSI da seguinte forma:

Figura 1 – Camadas do Modelo OSI

Fonte: estrategiaconcursos.com.br (2023).

1. Camada Física - Camada responsável pela transmissão física de dados, ela tem o objetivo de enviar sinais ou pulsos elétricos de uma máquina para outra sem se preocupar com as informações contidas ali. Ela se encarrega por definir a estrutura física da comunicação como cabos, conectores, tamanho e potência de antenas, ondas elétricas e aspectos de rede.

2. Camada de Enlace de Dados - Fornece uma interface que liga a camada física com a rede, é a principal responsável pela detecção de erros e correção, autorização de acessos e organização de dados. É a camada que garante uma transmissão de dados segura na rede local.

3. Camada de Rede - Tem a principal função de enviar pacotes de dados do remetente ao destinatário usando o roteamento, e assim procurando o melhor caminho possível para essa transmissão. Essa camada trabalha com endereçamento IP(Internet Protocol) para identificar dispositivos na rede e fazer o encapsulamento e endereçamento dos dados.

4. Camada de Transporte - Camada que tem a principal função de dividir e enviar pacotes para a camada de rede. Esta camada oferece comunicação segura entre a origem e destino e garante que todos os pacotes sejam entregues corretamente, lida também com retransmissão, caso haja alguma perda de dados ou corrupção de pacotes. Os firewalls tradicionais atuam apenas nessa camada, assegurando o tráfego de dados e bloqueando ou permitindo acesso a determinadas portas de origem e destino. Em geral, utilizam dois protocolos: TCP(Transmission Control Protocol) e UDP(User Datagram Protocol).

5. Camada de Sessão - Essa camada define o início e o fim das sessões de comunicação e gerencia a troca de dados entre dispositivos, ela permite o controle e sincronização entre as aplicações.

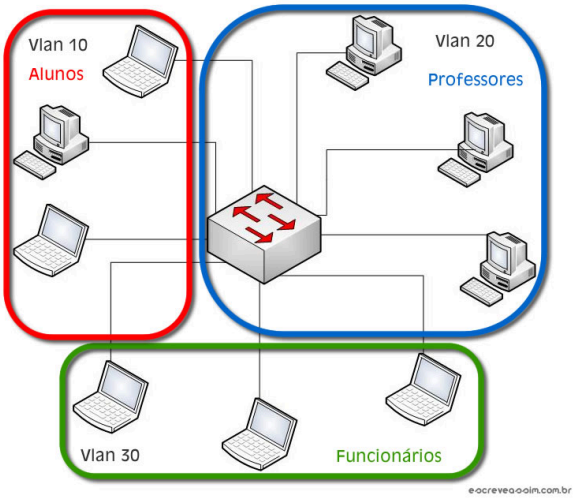
6. Camada de Apresentação - Esta camada garante que os dados sejam compreensíveis para as aplicações, ela realiza as funções de criptografia e descriptografia, conversão de formato de dados e tradução de caracteres. Além disso, permite que diferentes sistemas se comuniquem de forma transparente.

7. Camada de Aplicação - É a camada mais alta do modelo OSI, ela possibilita ao usuário que acesse e se comunique com outros serviços de rede e interajam com aplicativos em um nível mais alto. Nessa etapa, os NGFW fazem o inspecionamento desse tráfego, analisando e examinando os dados para saberem quais são os aplicativos que são permitidos na rede . Utilizamos protocolos específicos: HTTP, SMTP, FTP, DNS, DHCP, SSH, entre outros.

2.2 Vlan

O conceito de VLAN, (Virtual Local Area Network ou Rede Local Virtual) permite a divisão de uma rede física em outras segmentações de redes virtuais independentes, conforme Figura 2. Essa funcionalidade está ligada à camada 3 do modelo OSI.

Figura 2 - Vlan



Fonte: diegomacedo.com.br

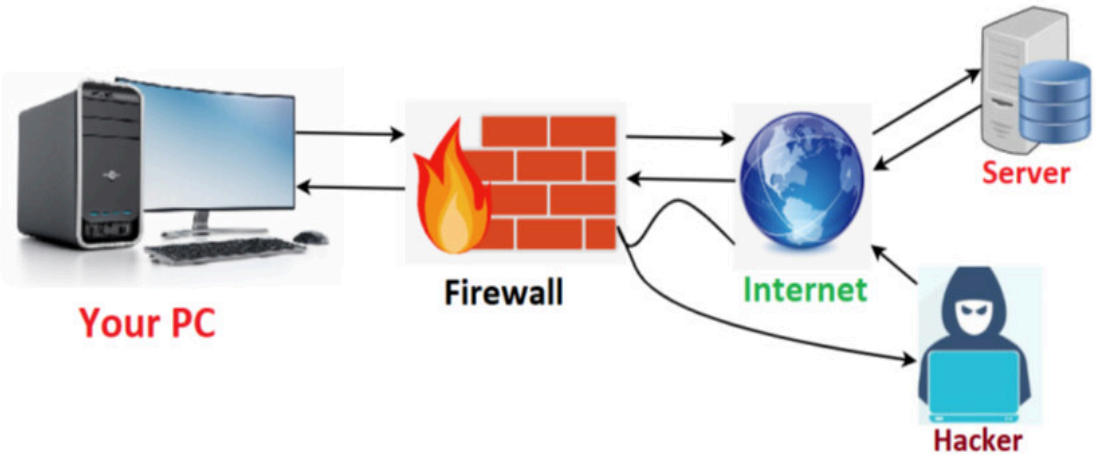
A ideia por trás dessa estratégia é a facilidade de gerenciamento, a segurança e a melhor eficiência da rede, pois, após a rede ser virtualizada e dividida, por meio de Switches, os dispositivos se mantêm na mesma rede local mas, como estão em Vlans diferentes, não podem se comunicar. Além disso, as VLANs entregam uma segurança mais eficiente e flexível, gerando uma maior facilidade no gerenciamento da rede, podendo fazer modificações, adicionar, remover e ainda mudar a topologia da rede, já que a VLAN é independente da estrutura física. As VLANs permitem aos administradores particionar suas redes para priorização de tráfego e o gerenciamento de acesso a recursos, dependendo da sua estrutura física.

2.3 Firewall

O firewall de rede é o principal responsável pela segurança, toda a configuração cabe ao administrador do sistema. Com a utilização do firewall, a rede recebe uma segurança extra, que tenta garantir o tráfego seguro de pacotes e a autorização de usuários para terem acesso à rede. Na figura 3 é possível visualizar que o firewall funciona como uma “parede de fogo”, tudo que passa por ele é supervisionado e verificado para saber se há alguma possibilidade de infiltração ou tentativa de acesso à rede.

Há dois tipos de firewalls: Firewall de Hardware e de Software. Sua utilização é importante para a proteção da rede de computadores, pois atua como a primeira linha de defesa. Essa barreira possui um conjunto de regras que podem ser inseridas pelo administrador da rede, que tem o total controle dos dados, uma das principais funcionalidades dos firewalls é a filtragem de pacotes, monitoramento de entrada e saída e permissão de tráfego.

Figura 3 - Firewall



Fonte: forumautomation.com

Como o foco principal é a segurança do ambiente em que o firewall está envolvido, há soluções que focam em garantir essa melhoria. Os firewalls de hardware tem esse único papel que nada mais é do que um equipamento que contém apenas essa ferramenta de segurança rodando, sua utilidade é mais indicada para médias e grandes companhias, porque são mais "parrudas" em questão de eficiência, e servem de suporte para os firewalls lógicos.

2.4 NGFW PfSense

O Pfsense é um firewall de código aberto que atualmente está na versão 2.7.2, e desempenha um grande tem um grande papel na segurança e gerenciamento de informações, lida também com roteamento e uma gama de funcionalidades que são ideais para empresas de pequeno e médio porte, o firewall possui também uma variada lista de recursos que podem ser adicionados através de downloads de pacotes permitindo assim a adição de funcionalidades de acordo com a necessidade do usuário.(SANTOS 2022).

Esse firewall se destaca por fazer parte dos NGFW e pela capacidade de se conectar a rede e fazer toda a análise de confiabilidade. Ele possui uma gama de configurações, e é o primeiro a fazer uma camada na rede e prevenir possíveis ataques e tentativas de quebra de segurança. É importante ressaltar que ele possui bastantes funcionalidades de alguns softwares pagos e pelo fato

de ser gratuito e com intuito de segurança e proteção, isso o torna bastante usado.(INDICCA.COM, 2023).

O objetivo do firewall é monitorar toda a rede e todo o tráfego que passa por ela, barrando assim, conteúdos perigosos e protegendo todos os dispositivos.(SANTOS, 2022). Portanto, o sistema também possui suporte NAT(Network Address Translation) que permite a mudança de endereços IP privados para públicos, e com isso, protegendo toda a topologia da rede de ataques externos, isso é de suma importância quando só tem uma rede e é utilizada por muitos usuários.

2.4.1 Servidor DHCP

Para a eficiência e segurança da rede, o PfSense conta com um servidor DHCP incluso ao firewall, para que haja uma maior facilidade tanto na parte de organização, quanto na distribuição de IPs aos dispositivos conectados à rede, é possível reservar IPs para destinados equipamentos e separar uma certa quantidade para dispositivos não autorizados. A distribuição é feita automaticamente e é garantido que um mesmo endereço não seja entregue duas vezes, certificando que não haja conflitos na rede.

Deste modo, o administrador pode fazer as configurações no Pfsense de forma que a rede fique centralizada e que assim tenha uma simplicidade na manutenção e na economia de tempo. Com todo esse controle a rede fica protegida de ameaças que envolvam endereçamento público.

2.4.2 NAT no PfSense

Se referindo a segurança de IPs, o NAT(Network Address Translation) assume uma grande responsabilidade de segura, pois, é encarregado de permitir a conexão de dispositivos internos com a internet, o NAT pega um ou um grupo de endereços privados e os transforma em endereços públicos, para que possam acessar a internet sem ter perigo de ter recepção ou acesso não autorizado a pacotes. O PfSense suporta todos os tipos de NAT e tem todo o controle de portas, possui também o monitoramento do NAT, caso um usuário acesse um site inapropriado que por algum motivo não foi barrado pelo firewall ou cometa um cibercrime, o indivíduo assumirá total responsabilidade do ato, e se houver problemas relacionados ao tráfego terá mais facilidade para fazer a manutenção da conectividade. O NAT tem um papel crítico na segurança e no controle da rede.

2.4.3 Virtual Private Network (VPN)

Para a segurança de tráfego na rede, o pfSense oferece três opções para conectividade de VPN, são elas:

OpenVPN: É um dos protocolos mais populares em questão de segurança e configuração, este protocolo é capaz de criar conexões de ponto a ponto, criptografia e autenticação do tráfego da rede. Se destaca pela flexibilidade e a capacidade de ser usado em diferentes sistemas.

PPTP: O PPTP (Point-to-Point Tunneling Protocol) é um protocolo mais antigo e simples em relação às outras VPNs, não é tão seguro e é usado mais quando a compatibilidade é mais importante que a segurança, é fácil de configurar e é suportado por sistemas mais antigos.

IPsec: O IPsec é muito importante, porque é um grupo de protocolos responsável pela segurança entre dispositivos de rede, ele faz a criptografia de pacotes de rede e faz a autenticação até a origem do pacote. Por meio de testes feitos em uma empresa, o IPsec se mostrou bastante importante para a segurança, e diminuiu bastante os gastos com outras VPNs (FERREIRA, 2013).

Nesse caso é possível observar que o PfSense disponibiliza além de um firewall riquíssimo, uma VPN que atende todos os requisitos para uma segurança eficaz. Na parte de monitoramento é permitido obter um relatório de todos os usuários conectados na VPN em tempo real, como também interromper uma conexão específica trazendo um controle maior para o administrador.

2.4.4 Load Balancing (Balanceamento de carga)

O Load Balancing é uma função crucial no PfSense, pois ela é responsável por automatizar a troca de links caso ocorra um gargalo na rede ou um link de internet tenha ficado offline. É a partir disso que ocorre uma distribuição equivalente entre várias interfaces, esse benefício faz com que a rede fique mais estável e o tráfego não fique lento. O administrador tem total controle sobre as configurações e a distribuição para a sua preferência e necessidades.

2.4.5 Ponto de Acesso Wireless

O pfSense em si não faz o roteamento de uma rede wireless, mas é possível fazer essa extensão da rede por meio de um roteador que é conectado à porta LAN(Rede de Área Local) do PC que está com o sistema do PfSense. O administrador da rede faz a configuração do access point para todo o tráfego passar pelo PfSense, permitindo que dispositivos sem fio se conectem à rede local e, consequentemente, à Internet, quando configurado. O pfSense desempenha um papel importante ao rotear o tráfego entre dispositivos sem fio e a rede local, além de oferecer recursos avançados de segurança e controle de acesso, tudo que passa por ele é diagnosticado. Isso é essencial para controle de rede e organização.

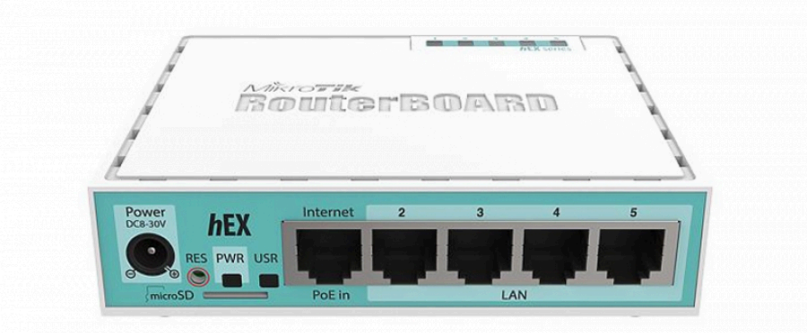
2.4.6 Reporting and Monitoring (Relatório e Monitoramento)

No pfSense é possível gerar relatórios de monitoramento da rede para obter informações sobre o desempenho, o tráfego e a utilização da rede. Os relatórios de monitoramento podem incluir informações de status da interface, gráficos de uso de largura de banda, logs do sistema, detalhes sobre conexões VPN, informações de autenticação, registros de DHCP e informações sobre conexões de firewall. Esses relatórios são de suma importância para verificar o funcionamento da rede, solucionar problemas e tomar decisões a partir dos dados sobre o gerenciamento da infraestrutura de rede.

2.5 Mikrotik Routerboard 750 Gr3

Os produtos MikroTik são usados em uma variedade de cenários, desde redes domésticas até redes empresariais de grande porte. Esses aparelhos são populares devido à sua escalabilidade e capacidade de atender a um grande número de clientes. Na figura 4 é possível analisar toda sua parte física e como ele favorece a estrutura da rede em questão de redundância e organização.

Figura 4 - Mikrotik RB750 Gr3



Fonte: itwarehouse.ph

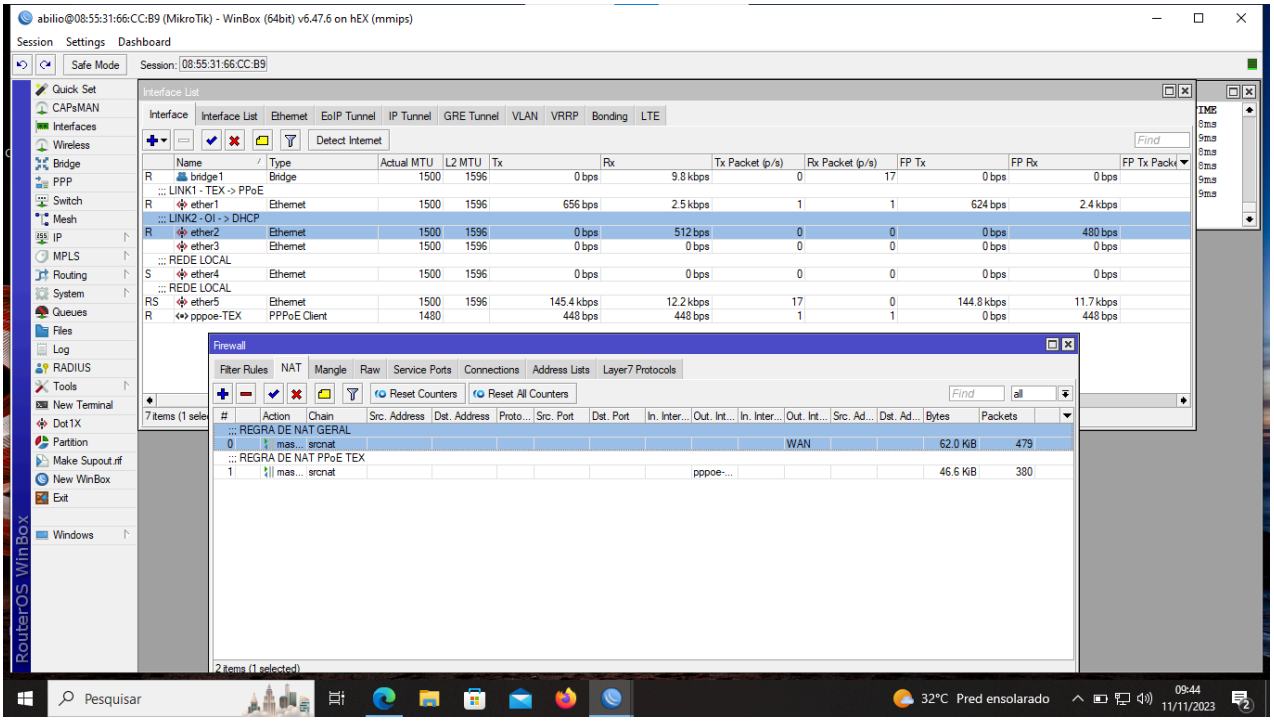
Esse aparelho tem grande espaço no mercado pela sua capacidade de receber até quatro links de internet e enviar um link para a rede local totalmente balanceado, com isso, a rede nunca ficará offline. Seu preço também chama muita atenção, porque sua capacidade de eficácia é ótima.

A principal característica destes roteadores, além da sua ampla flexibilidade de uso, é também a possibilidade que o administrador da rede tem de total controle. O Mikrotik é um sistema completo, com todas as ferramentas necessárias para roteamento dinâmico ou estático, para criação de VPNs e possui firewall completo com todas as funcionalidades necessárias para marcação de pacotes, bloqueios e controle de acesso.

2.6 Winbox

O winbox é uma ferramenta de fácil acesso e foi criada pela Mikrotik. Normalmente é usada no windows, se surgir a urgência de usar em linux, é necessário a instalação de um emulador. Essa ferramenta dá acesso às configurações de suas necessidades(Servidores, RouterBoard e demais equipamentos Mikrotik), pode-se administrar todo o ambiente, incluindo as regras de firewall, através de uma interface gráfica, sua utilização é importante porque diminui o tempo que levaria para fazer todas essas configurações separadamente via linha de comando. Como é mostrado na figura 5.

Figura 5 - Interface do Winbox



Fonte: Autoria própria

Na interface winbox foi aberta duas janelas: Uma de interface de rede onde é possível ter acesso aos seus dados e informações sobre o link de internet que está chegando no mikrotik, e a outra janela com a regra de NAT geral para possível acesso a internet.

3 METODOLOGIA DA PESQUISA

A metodologia utilizada foi baseada no estudo de caso de dois firewalls de nova geração, o PfSense e o Mikrotik RouterBoard 750 Gr 3, que são bastante utilizados e pelo fato de um deles ser gratuito e ter uma comunidade ativa e bem organizada, que é o caso do PfSense, e o Mikrotik, que é bem visto pela sua utilização e por conseguir suprir as necessidades de uma rede de computadores e manter o gerenciamento de acordo com suas configurações .

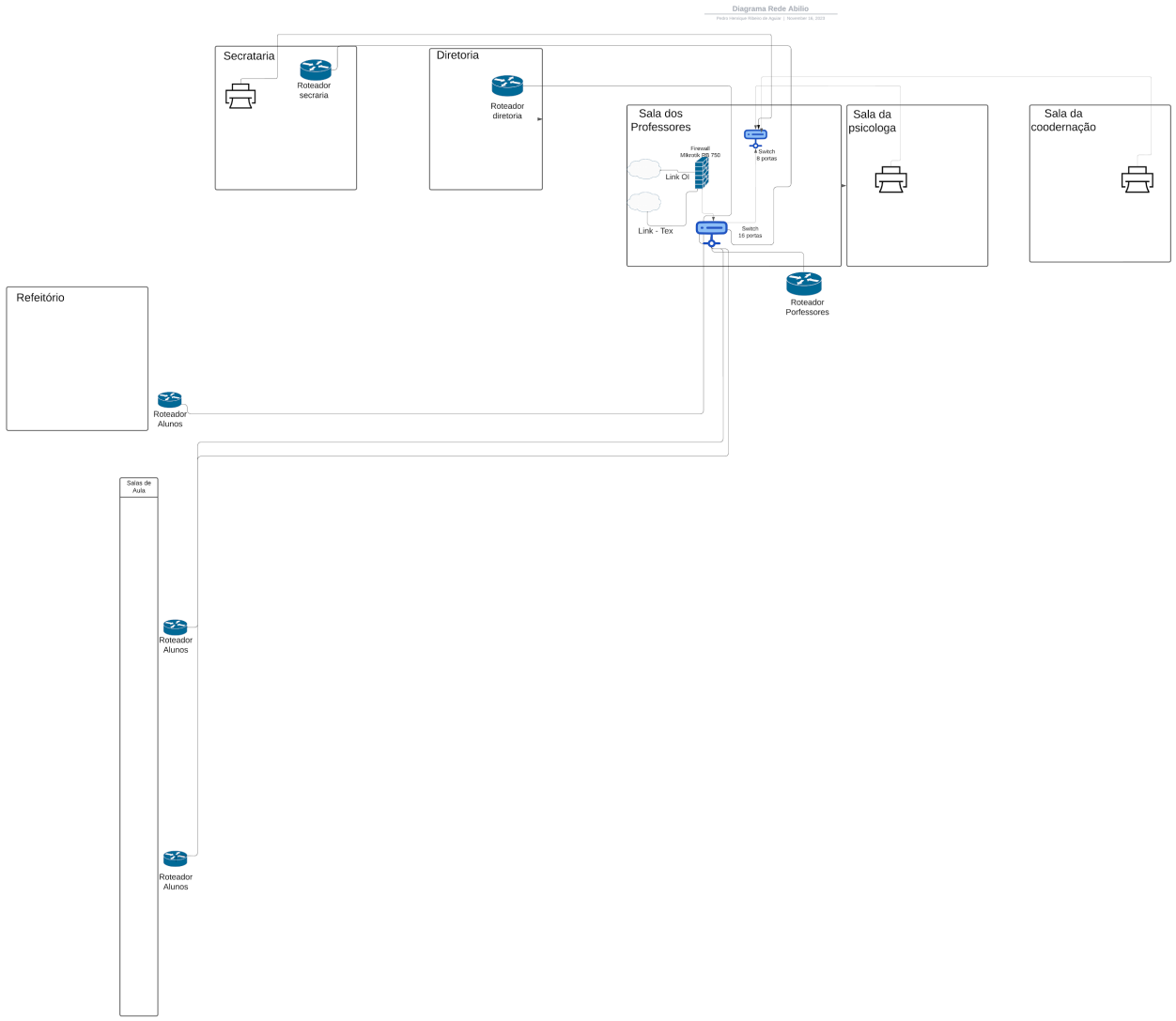
3.1 Análise da Rede

De início, o projeto tinha como objetivo a implementação do PfSense na Escola Estadual Coronel Abílio Wolney para uma nova estruturação da rede, que não contava com um bom funcionamento. Foi feito um balanço geral das máquinas da instituição, e o resultado não foi muito satisfatório, porque os equipamentos de hardware obsoleto não iriam conseguir processar o PfSense. Diante disso, foi marcada uma reunião com a Diretoria da escola para saber qual o meio mais viável para concluir o projeto.

Logo após a reunião, concluiu-se que deveria ser feito um orçamento para analisar qual dos equipamentos seria preciso comprar. Depois de muitas pesquisas e cálculos com base no orçamento da escola e que as máquinas que estavam lá não eram capazes de processar o PfSense , foi constatado que a melhor forma seria utilizar o Mikrotik RouterBoard 750 Gr 3, que contava com um preço satisfatório e que se encaixava no orçamento desejado.

Depois da compra do equipamento e início das configurações no mesmo, o projeto começou a fluir para um bom resultado. Foi levado em consideração regras que seriam eficientes para não deixar a internet com gargalos e com muita latência, e um gerenciamento que iria favorecer a rede para uma melhor entendimento. Caso fosse necessário uma manutenção, a distribuição da rede foi feita por meio de *access points* para os setores administrativos e uma rede livre para os alunos, são elas: Rede da Secretaria, Rede dos Professores e a rede aberta para os Estudantes. Na figura 6 é mostrado todo o diagrama da rede da Escola Abílio Wolney, os pontos onde foram colocados os equipamentos beneficiam os setores ao lado, tornando assim, toda a escola conectada.

Figura 6 - Diagrama da Rede da Escola Estadual Abílio Wolney



Fonte: Autoria própria

4 IMPLEMENTAÇÃO E ANÁLISE

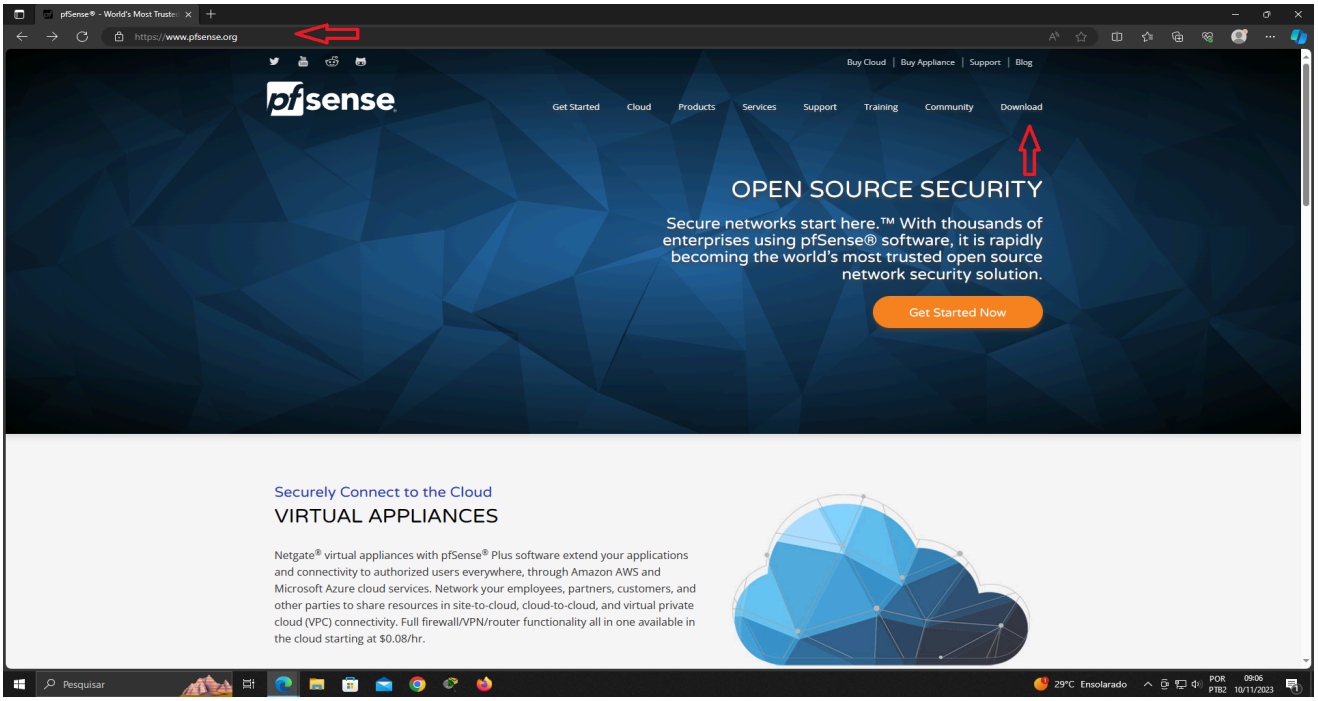
Esta seção tem como objetivo apresentar as etapas seguidas e os resultados obtidos, a fim de identificar os pontos positivos e negativos. Dentre os fatores importantes deste trabalho, estão a alta disponibilidade, baixo investimento que são os principais para sua elaboração.

Os testes do PfSense foram feitos em uma VM(Máquina Virtual) que facilita a análise e funcionamento do firewall.

4.1 Tutorial de Instalação do PfSense

Para fazer a instalação do PfSense, primeiro é necessário entrar em um navegador e acessar o seguinte link: [pfSense® - World's Most Trusted Open Source Firewall] que vai exibir todas as informações sobre o site do PfSense e o caminho de direcionamento de download, assim como mostra a figura 7 a seguir:

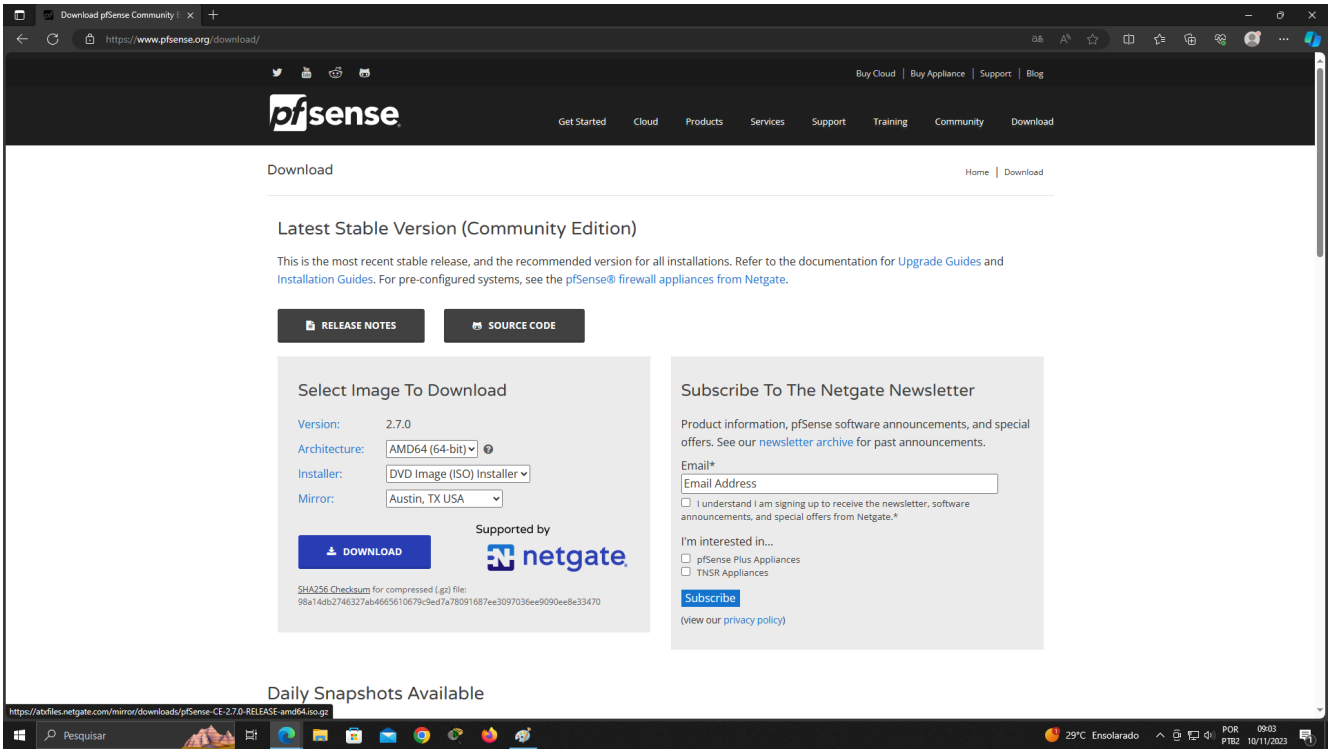
Figura 7 - Site de acesso ao PfSense



Fonte: Autoria própria.

É importante ressaltar que o PfSense deve ser baixado em imagem ISO mais recente para ser instalado na máquina virtual assim como mostra na figura 8 abaixo:

Figura 8 - Download da imagem ISO Pfsense



Fonte: Autoria própria.

Após o download da ISO, devem ser seguidos uma sequência de passos para a conclusão da instalação e utilização do PfSense, assim como mostra o link a seguir: Instalação de PFSense como Gateway de sua rede. - Made4It. O autor deixa explícito cada passo a ser seguido desde a instalação do Firewall, até a configuração no terminal do PfSense, e por fim, como é inserido o IP da rede e algumas regras de firewall .

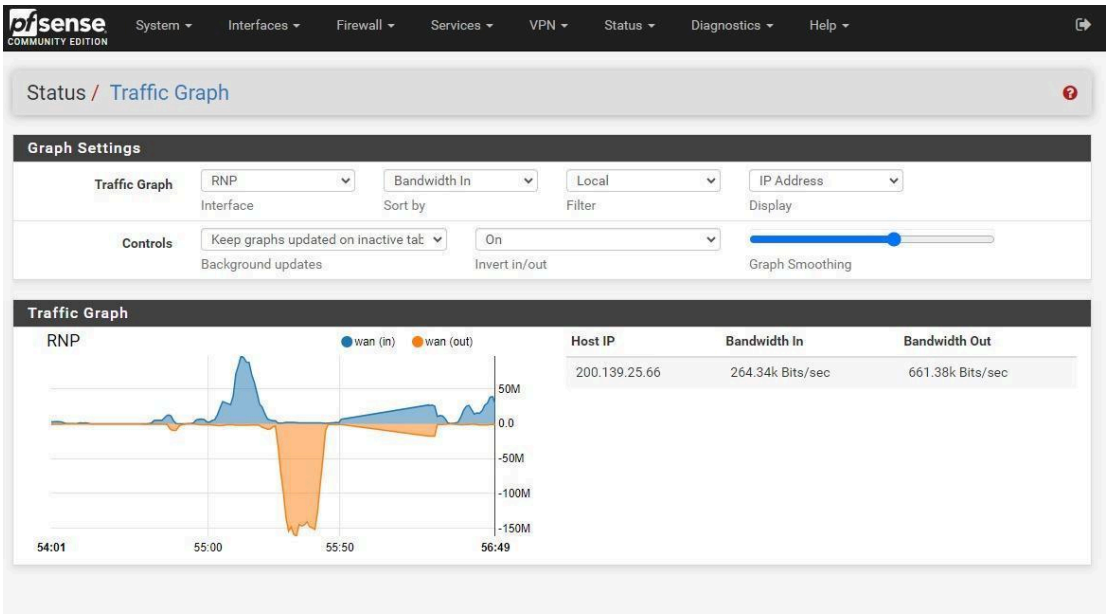
4.1.1 Analisando a funcionalidade do gráfico de monitoramento

O gráfico de monitoramento do pfSense oferece uma visão abrangente do desempenho da rede e do sistema. Alguns dos principais elementos que você pode encontrar nos gráficos de monitoramento incluem:

- Utilização de CPU e Memória;
- Utilização de interface de rede;
- Conexões ativas;
- Latência e perda de pacotes;

A análise testada foi com gráfico de interfaces de rede, como mostra a figura 9 a seguir:

Figura 9 - Análise da interface de rede 1

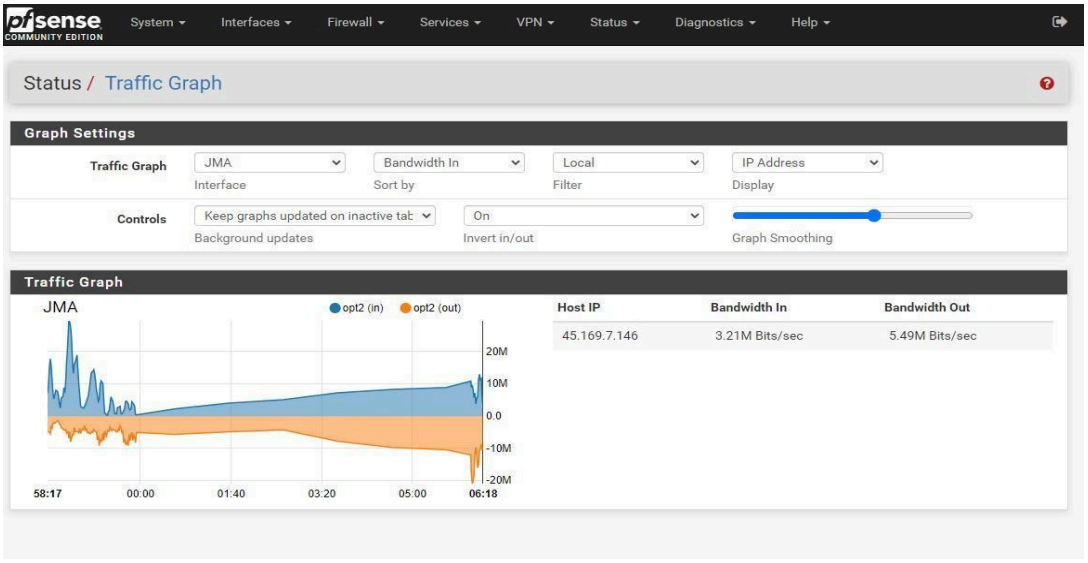


Fonte: Autoria própria.

Essa imagem descreve como está sendo a utilização da rede que é usada como principal na instituição para gerenciamento da rede.

A figura 10 também traz como foco o consumo da interface de rede que fica como link secundário, caso a rede tenha perda de um sinal de internet.

Figura 10 - Análise da interface de rede 2

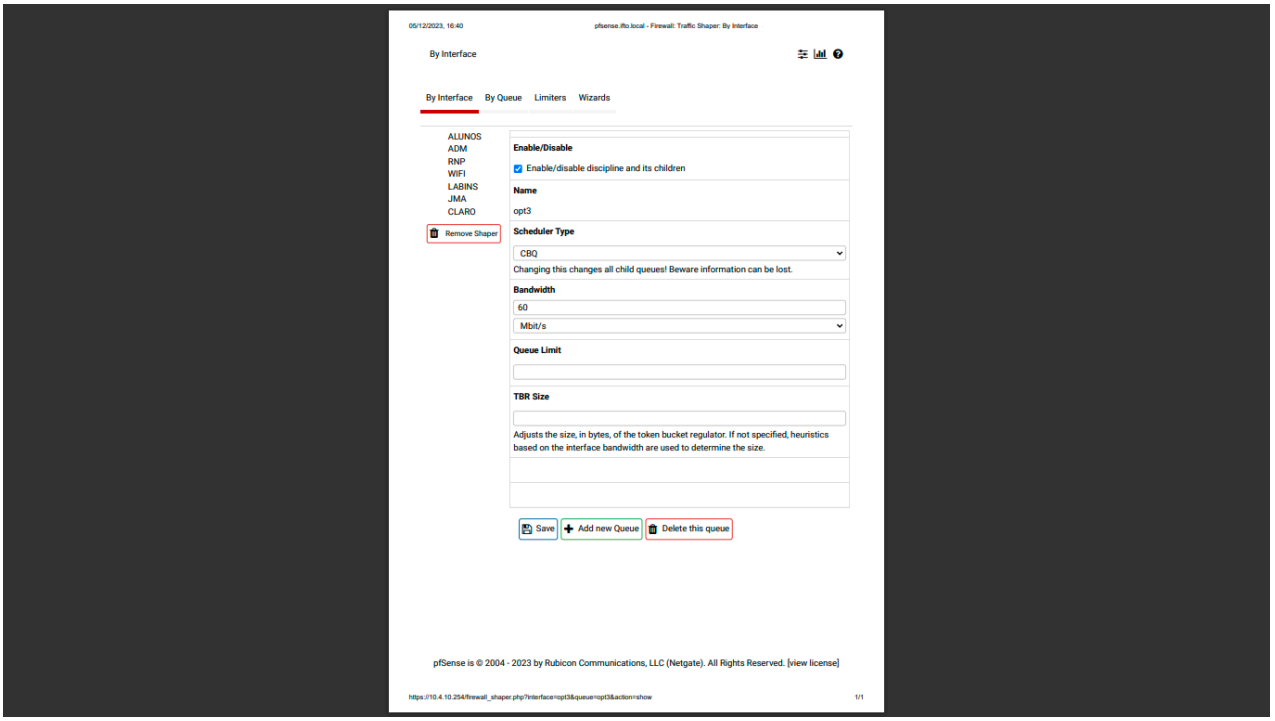


Fonte: Autoria Própria

4.1.2 Implementando a funcionalidade de balanceamento

O balanceamento que foi testado no PfSense, conta com o consumo de um link primário, que atende uma demanda maior, e um link secundário para um consumo mínimo, e que também é usado como failover, que é quando o link principal fica offline e o secundário assume a conexão até o outro voltar. na figura 11 é mostrado a seguir a regra de balanceamento com divisão para uma rede lan dos acadêmicos:

Figura 11 - Análise da regra de balanceamento na rede LAN



Fonte: Autoria Própria

Na imagem mostrada, é possível analisar que a rede tem um balanceamento aplicado para os alunos na questão do consumo de internet, e que possui um consumo aceitável pelo fato de ter uma boa quantidade de estudantes e isso já evita o risco de congestionar a rede com muitos logs e acabar derrubando a mesma.

4.2 Tutorial de Configuração do Mikrotik

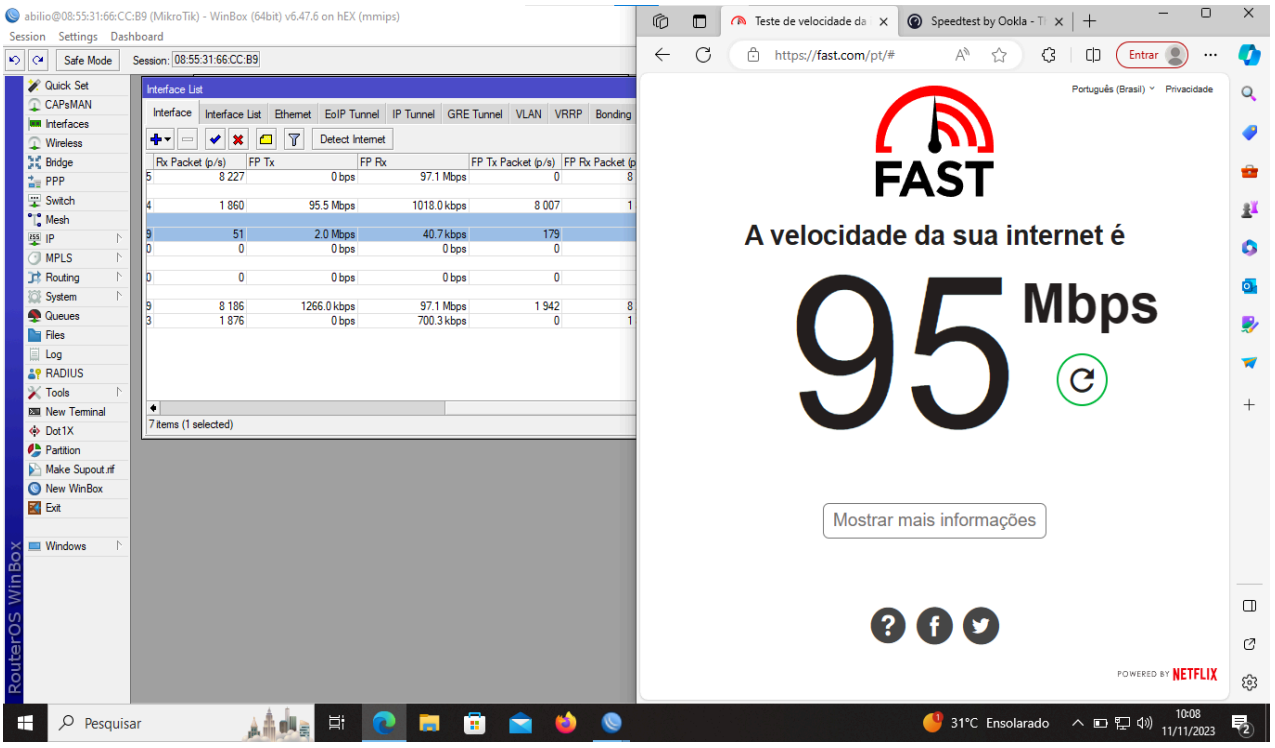
O Mikrotik foi escolhido pelo fato do seu preço ser acessível, pelo seu sistema e alto desempenho os aparelhos RouterBoard são conhecidos pelo seu tamanho compacto, eficiência energética, versatilidade em aplicações de rede e sua facilidade de configuração.

No link a seguir foi exibido todo o caminho percorrido até a conclusão da instalação e configuração: Tutorial básico para instalação Mikrotik - Redes e Internet - Clube do Hardware.

4.2.1 funcionalidade Balanceamento

A funcionalidade de balanceamento foi aplicada no mikrotik utilizando duas redes distintas, essa ação favoreceu a utilização mais eficiente da internet e proporcionou uma melhoria tanto na parte de navegação, quanto na segura, é possível observar que o Winbox mostra a utilização das duas redes no momento do teste de velocidade, assim como mostra a figura 12 .

Figura 12 - Balanceamento de duas interfaces de rede no Mikrotik

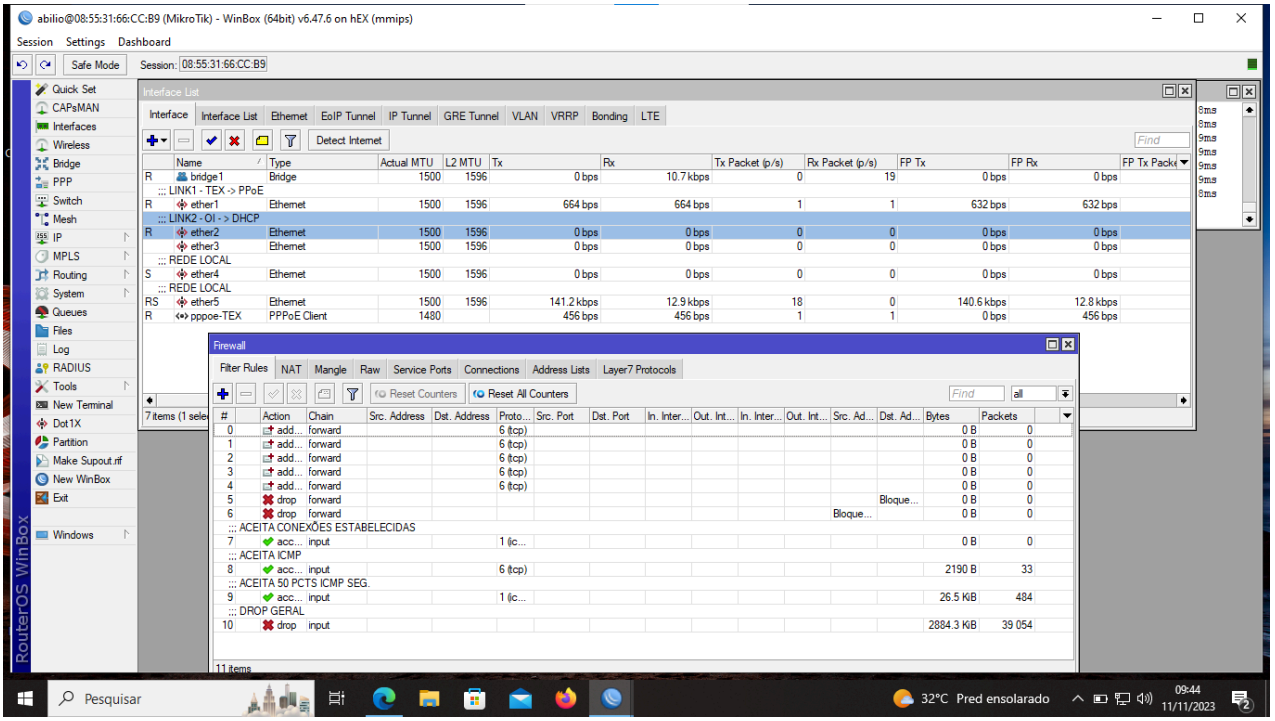


Fonte: Autoria Própria

4.2.2 Implementando a Funcionalidade de Bloqueio de Sites e Drop

Foi implementado no firewall RB Mikrotik algumas funções para a segurança da rede e do aparelho, dentre essas configurações, estão: Bloqueio de sites inapropriados, Drop de pacotes que contenham alguma tentativa de invasão ao sistema e Drop geral, aceitação de conexões relacionadas e demais configurações, assim como mostra a imagem 13.

Figura 13 - Bloqueio de Sites inapropriados e Drop de Pacotes



Fonte: Autoria Própria.

4.3 Análise

O pfSense, como uma solução de código aberto, oferece vantagens econômicas e um suporte ativo por meio da comunidade. Sua interface gráfica intuitiva facilita a configuração e administração, tornando-o acessível mesmo para usuários menos experientes. Além disso, a capacidade nativa de suportar VPNs permite conexões seguras entre diferentes locais, enquanto seu firewall robusto, com recursos avançados de filtragem e monitoramento em tempo real, contribui para a segurança da rede, isso o torna um firewall de nova geração que atende muitas demandas necessárias na rede

Entretanto, é importante considerar que o pfSense pode exigir hardware mais potente para um desempenho ideal, por esse motivo ele foi instalado em uma VM para testes, pois a Escola Coronel Abílio Wolney onde o foi feito o projeto não tinha muitos recursos para máquinas potentes que suportariam o sistema do PfSense rodando, especialmente em um ambiente como a escola, onde tem um grande número de usuários.

No que diz respeito ao MikroTik, sua característica de custo-benefício é notável, entregando assim um dispositivos mais acessíveis e eficientes para um bom gerenciamento. A flexibilidade de configuração é uma vantagem significativa, porque ele oferece uma variedade de recursos e opções adequadas para redes de diferentes tamanhos, e suas ferramentas de monitoramento detalhado fornecem feedbacks valiosos sobre o tráfego e o desempenho da rede.

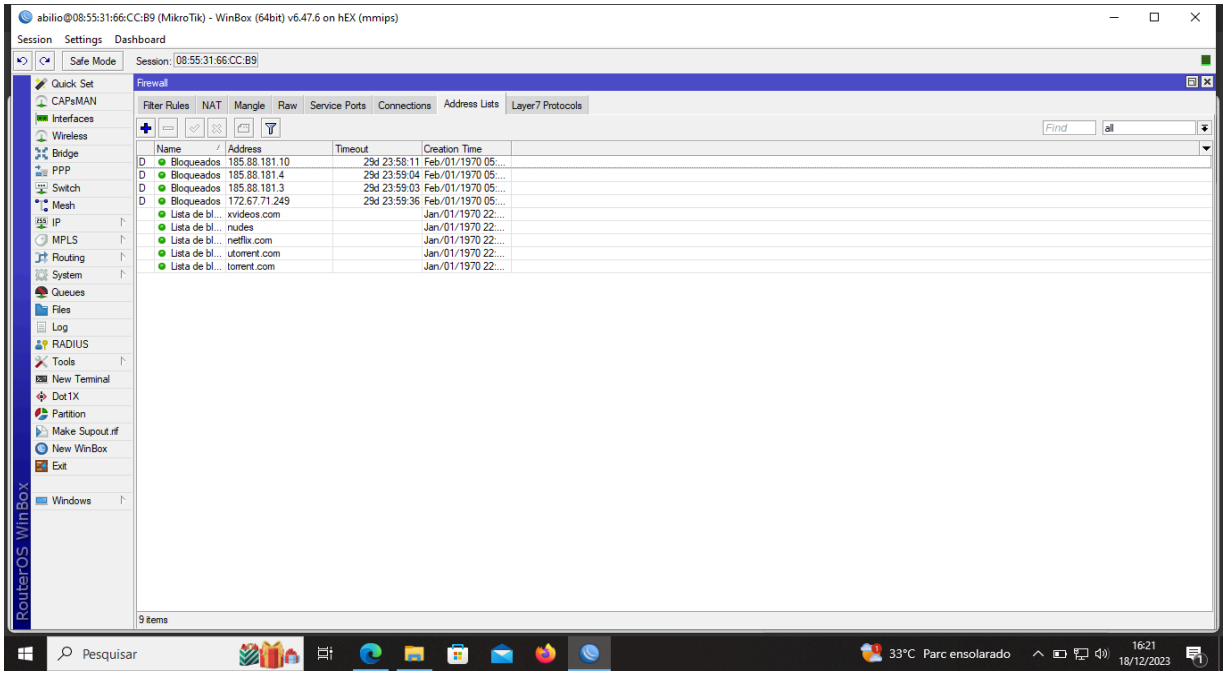
Ambas as soluções apresentam vantagens e desafios, e a escolha entre pfSense e MikroTik dependerá das necessidades específicas e do administrador responsável pelo gerenciamento da rede.

4.4 Testes das Regras de Firewall Mikrotik Routerboard 750 Gr 3

As regras foram feitas corretamente no equipamento MikroTik RB750 para garantir a segurança da rede escolar, foram estabelecidas políticas de segurança padrão para certificar todo o tráfego de entrada e saída e permitir apenas comunicações que sejam eficientes para as operações educacionais.

A filtragem de conteúdo também desempenha um papel vital na segurança escolar, bloqueando o acesso a sites inadequados ou irrelevantes e assim, facilitando o monitoramento e o tráfego da rede, como é exibido na figura 14.

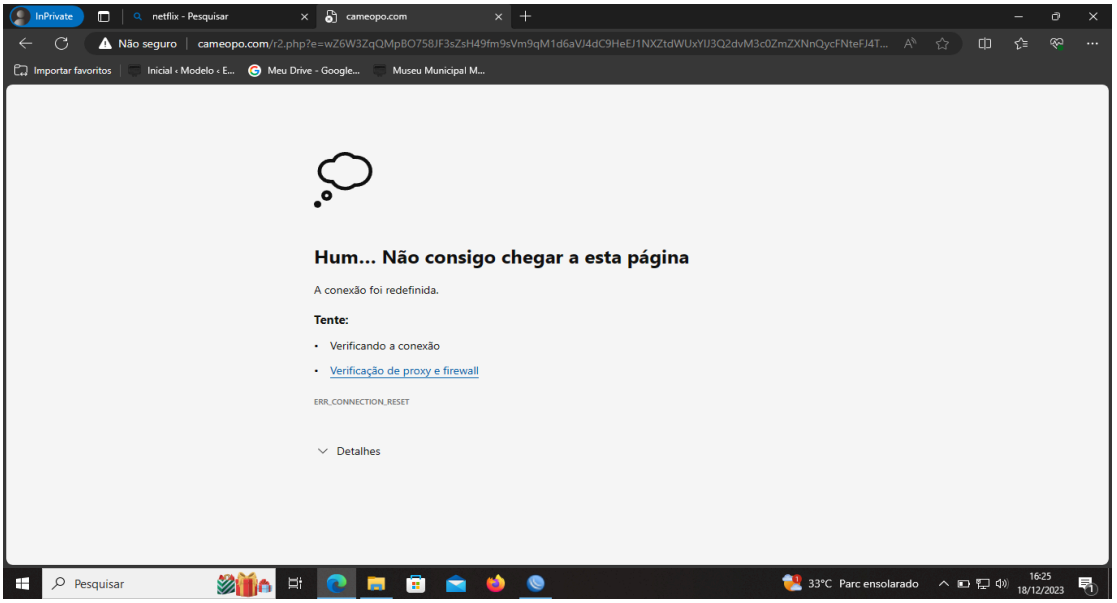
Figura 14 - Resultado das regras de Firewall na RB 750 Gr 3



Fonte: Autoria própria

É possível analisar a imagem e verificar que os sites foram dropados e o Mikrotik continua com os IPs para continuar fazendo o drop desses pacotes que seriam entregues ao usuário, caso eles tentem fazer esse envio novamente. Na imagem abaixo é mostrado que na tentativa de fazer o acesso a própria netflix, o site já não é permitido e não consegue enviar seus pacotes ao usuário final, assim como mostra a figura 8.

Figura 15 - Drop do site da Netflix



Fonte: Autoria própria.

5 CONSIDERAÇÕES FINAIS

O desenvolvimento do presente trabalho possibilitou a análise e aplicação de elementos para promover a segurança da informação em um ambiente de rede de computadores da rede escolar Coronel Abílio Wolney, utilizando o aparelho Mikrotik RouterBoard 750 Gr3 e suas ferramentas, e fazer testes com o PfSense e suas metodologias apresentadas neste estudo. Além disso, o estudo foi realizado utilizando-se várias referências bibliográficas, apresentando como os recursos podem ajudar a promover a segurança e o melhor gerenciamento da rede.

O principal objetivo do presente trabalho foi demonstrar ambas as utilizações do Mikrotik e do PfSense que é um software livre da área de segurança, de caráter de gratuidade, eficaz e objetivos e ter a utilização e proteção de suas informações digitais, ou seja, sua necessidade gerencial de uma política de segurança.

Os principais resultados se referem a função de firewall do referido software livre, isto é, a possibilidade dele bloquear todo e qualquer tipo de acesso que possua um caráter duvidoso, fazer uma varredura completa na rede para evitar acessos não desejados e pela possibilidade de evitar um ataque cibernético. Como pôde ser observado no desenvolvimento e resultados. A utilização do Mikrotik RouterBoard 750 Gr3 e sua Política de Segurança da Informação documentada, tiveram resultados satisfatórios, comprovando a segurança das informações da organização, tendo assim um ótimo resultado final no projeto.

REFERÊNCIAS

Cert Br. **Cartilha de Segurança para Internet**. Disponível em: <https://stats.cert.br/incidentes/>. Acesso em: 18 set. 2023.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**. 5. Ed. São Paulo, 2009. Disponível em: <https://www.facom.ufu.br/~sequincozes/referencias/kurose2010.pdf>. Acesso em: 11 set. 2023.

Made4It. (2020). **Instalação de PfSense como Gateway de sua rede**. Disponível em: <https://made4it.com.br/instalacao-de-pfsense-como-gateway-de-sua-rede/>. Acesso em 13 Nov. 2023.

pfSense Documentation. **Thoroughly detailed information and continually updated instructions on how to best operate pfSense® software**. Disponível em: <https://docs.netgate.com/pfsense/en/latest/>. Acesso em: 18 set. 2023.

Programadores Depre. (2023). **Como garantir a segurança da rede de computadores da sua empresa**. Disponível em: <https://programadoresdepre.com.br/como-garantir-a-seguranca-da-rede-de-computadores-da-sua-empresa/>. Acesso em: 11 set. 2023.

STORAGE JÁ. (2023). **Rede de Computadores - O Guia completo 2023!**. Disponível em: <https://www.storageja.com.br/post/rede-de-computadores>. Acesso em: 11 set. 2023.

TANENBAUM, Andrew S. **Redes de Computadores**. (1996). Disponível em: <http://www-usr.inf.ufsm.br/~rose/Tanenbaum.pdf>. Acesso em: 11 set. 2023.

Winbox. **Router OS - Mikrotik**. Disponível em: <Winbox - RouterOS - MikroTik Documentation>. Acesso em: 07 Nov. 2023.

4.Linux. **O que é o PfSense - Seus principais recursos**. Disponível em: <https://4linux.com.br/o-que-e-pfsense/>. Acesso em: 19 Set. 2023.