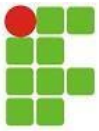


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA
E TECNOLOGIA DO AMAPÁ – IFAP
CÂMPUS MACAPÁ
CURSO SUPERIOR TECNOLOGIA DE REDES DE COMPUTADORES

RAIANDERSON DE OLIVEIRA BARROSO

PFSENSE:
Teletrabalho durante a Pandemia do Covid-19

MACAPÁ - AP
2021

RAIANDERSON DE OLIVEIRA BARROSO

PFSENSE:

Teletrabalho durante a Pandemia do Covid-19

Trabalho de conclusão do curso apresentado ao Curso Superior Tecnologia de Redes de Computadores, do Instituto de educação, ciência e tecnologia do Amapá – IFAP, como requisito obrigatório para obtenção do grau de Tecnólogo em Redes de Computadores.

Orientador (a): Célio do Nascimento Rodrigues

MACAPÁ - AP

2021

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

B277p Barroso, Raianderson de Oliveira.
Pfsense: Teletrabalho durante a pandemia do covid-19 / Raianderson de Oliveira Barroso - Macapá, 2021.
43 f.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2021.

Orientador: Me. Célio do Nascimento Rodrigues .

1. Pfsense. 2. Teletrabalho. 3. Redes de Computadores. I. , Me. Célio do Nascimento Rodrigues, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

RAIANDERSON DE OLIVEIRA BARROSO

PFSENSE:

Teletrabalho durante a Pandemia do Covid-19

Trabalho de conclusão do curso apresentado ao Curso Superior Tecnologia de Redes de Computadores, do Instituto de educação, ciência e tecnologia do Amapá – IFAP, como requisito obrigatório para obtenção do grau de Tecnólogo em Redes de Computadores.
Orientador (a): Célio do Nascimento Rodrigues

BANCA EXAMINADORA

_____

Prof. Me. Célio do Nascimento Rodrigues

_____

Prof. Esp. André Luiz Simão de Miranda

_____

Prof. Esp. Lourival Queiroz Alcântara Júnior

Aprovada(o) em: 09/06/2021

Nota: 8.0

AGRADECIMENTOS

Primeiramente quero agradecer a Deus por me dar saúde, sabedoria, e principalmente por cuidar da minha família durante essa situação em que o mundo vive em 2021. A minha família que sempre me apoiou emocional e financeiramente durante longos anos nesse curso. Aos docentes do IFAP que estiveram presentes ao longo curso, em especial ao professor Célio Rodrigues, pela orientação, paciência em explicar o funcionamento do trabalho desde sua criação e pelo tempo dedicado em ensinar matérias relacionadas redes de computadores. Além disso, meus agradecimentos a todos os funcionários da Secretaria de Tecnologia da Informação (STI) do Tribunal Regional Eleitoral, em especial ao subsetor da Coordenadoria de Soluções Corporativas (Leonardo, Davi, Soraya, Wainner Caetano e Junior).

RESUMO

Tendo em vista que a ferramenta possui grande número de aplicações e que estas oferecem diversos benefícios para os usuários em geral, pesquisa-se sobre o Pfsense como solução para teletrabalho durante a pandemia do Covid-19. Para tanto, é necessário abordar as principais funcionalidades e vantagens, a implantação de uma rede análoga, configuração dos serviços remoto e as aplicações utilizadas nas empresas. Realiza-se, então, uma pesquisa bibliográfica, baseando-se em matérias digitais, pesquisas acadêmicas e livros sobre o assunto, e uma pesquisa explicativa, a fim de explicar conceitos relacionados ao assunto estudado. Diante disso, verifica-se que o software possibilita o administrador de rede gerenciar uma infraestrutura com mecanismos de fácil configuração e manutenção e o uso de soluções de acesso remoto para auxiliar na continuação e produtividade da empresa, o que impõe a constatação de que os serviços oferecidos pelo servidor Pfsense cumpre o papel manter a conectividade e fluidez na comunicação dos usuários das organizações durante a pandemia da covid-19.

Palavras-chave: Pfsense. Acesso Remoto. Teletrabalho. Redes de Computadores. Software Livre.

ABSTRACT

Considering that the tool has a large number of applications and that these offer several benefits to users in general, research is being carried out on Pfsense as a solution for teleworking during the Covid-19 pandemic. Therefore, it is necessary to address the main features and advantages, the implementation of an analogous network, configuration of remote services and applications used in companies. Then, a bibliographical research is carried out, based on digital materials, academic researches and books on the subject, and an explanatory research, in order to explain concepts related to the studied subject. Therefore, it appears that the software enables the network administrator to manage an infrastructure with mechanisms for easy configuration and maintenance and the use of remote access solutions to assist in the continuation and productivity of the company, which imposes the verification that the services offered by the Pfsense server fulfills the role of maintaining connectivity and fluidity in the communication of users of organizations during the covid-19 pandemic.

Keywords: Pfsense. Remote access. Telework. Computer network. Free Software.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Segundo a OPAS (2021), a Covid-19 é uma doença altamente transmissível provocada pelo coronavírus (SARS-CoV-2). Em 2019, causou uma mudança radical no modo das pessoas se relacionarem e também trabalharem, criando assim um novo desafio para diversas áreas que movimentam o mercado financeiro, como por exemplo a empresarial. Segundo pesquisa CETICBR (2020), durante a pandemia houve aumento no uso de ferramenta para teletrabalho, com 46% no acesso remoto de pastas e arquivos das empresas e 37% no uso de softwares, o que evidencia a importância das tecnologias capazes de auxiliar no dia a dia de um funcionário durante esse período.

A complexidade das infraestruturas de rede foi ampliada, gestores da área precisam lidar com um parque tecnológico que possui múltiplos sistemas como servidores e serviços em geral. Nesse contexto, destaca-se o firewall Pfsense que possui rol de funções de gerenciamento e controle de fluxo das informações trafegadas pela rede, bem como fornece acesso remoto de servidores locais aos usuários e administradores. Assim, essa ferramenta é útil nas organizações, pois pode ser uma solução de alta qualidade para acesso aos serviços de rede interna e eventualmente diminuir os custos financeiros no setor tecnológico.

Na primeira parte será apresentado, como fundamento teórico, conceitos acerca do software bem como seus principais benefícios.

Por sua vez, a segunda parte apresentará a implementação do Pfsense em uma rede cliente servidor, mostrando passo a passo da sua instalação e configuração.

Por fim, a terceira parte mostrará o funcionamento do firewall com uso remoto, usando um servidor MYSQL e SAMBA para consulta de dados e compartilhamento de arquivos, respectivamente.

2 JUSTIFICATIVA

O Pfsense é um firewall que delimita uma rede local da internet por meio de regras e funções de controle. Sua licença é baseada na BSD, utilizada em programas de código aberto e de livre distribuição, o que permite ser distribuído gratuitamente na internet. Além disso, destaca-se sua função de centralizar diversos serviço e ferramentas para auxiliar na segurança e no gerenciamento das informações trafegada pelo firewall, como servidores (DHCP, DNS, VPN, PPOE e etc.), proxy, firewall, IDS/IPS e entre outros.

Com seu uso, empresas podem desfrutar de uma ferramenta para gerenciar o controle de usuários, clientes, bem como aumentar a produtividade desses com as tecnologias empregadas na internet.

Assim, o que impulsionou o desenvolvimento deste trabalho foi apresentar Pfsense como uma ferramenta que pudesse solucionar o uso de teletrabalho durante a pandemia em empresas de pequeno porte, pois ele possui ampla funções e serviços que auxiliam no controle e acesso remoto da rede dessas empresas. Desse modo, foi apresentado conceitos, definições e a implementação do Pfsense, baseando-se nos entendimentos de autores da área e no conhecimento adquirido durante o curso.

3 OBJETIVOS

3.1 Geral

Apresentar o firewall Pfsense como solução de trabalho remoto para pequena empresa durante a pandemia.

3.2 Específicos

- Levantar as principais funcionalidade e vantagem do PfSense;
- Elaborar um ambiente tecnológico semelhante de uma empresa;
- Instalar e configurar Pfsense;
- Configurar servidor com OpenVPN;
- Testar o uso remoto com uso do SAMBA e MySQL.

4 METODOLOGIA DE PESQUISA

O tipo de metodologia aplicada neste trabalho foi a pesquisa bibliográfica e a pesquisa explicativa. Segundo o autor Gil (2008), a primeira é desenvolvida por meio de material elaborado, incluindo livros e artigos científicos. Sua principal vantagem está no fato de permitir investigar um número amplo de fenômenos que outras pesquisas.

Ainda, segundo o autor Gil (2008), a pesquisa explicativa tem a preocupação em identificar fatores que contribuem para a ocorrência dos fenômenos. Ela estuda a realidade de uma forma mais aprofunda, explica quais razões e os porquê que as coisas acontecem.

5 FUNDAMENTAÇÃO TEÓRICA

5.1 História do Pfsense

O Pfsense é um sistema operacional gratuito e de código aberto que foi baseado do FreeBSD para ser usado como firewall e roteador acessível e gerenciável por interface web. Ele possui uma lista de recursos e um repositório que permite adicionar extensões sem que atinja a vulnerabilidade dessa distribuição (PFSENSE, 2021).

Esse sistema tem como base o projeto m0n0wall, desenvolvido a partir do sistema operacional FreeBSD. Foi desenvolvido em setembro de 2004 por Chris Buechler e Scott Ullrich para criar um firewall completo para ser usado com PC integrado, fornecendo todos recursos essenciais de firewall comercial por um preço de software gratuito (WILLIAMSON, 2012).

5.1.1 Funções e Vantagens

a) Software baseado em Open Source

FreeBSD é um sistema operacional que permite a criação e a distribuição de sistema operacional licenciado pela BSD, o qual poderá ser adquirido gratuitamente, sem a necessidade de pagamento adicional de licença para uso (FreeBSD, 2021).

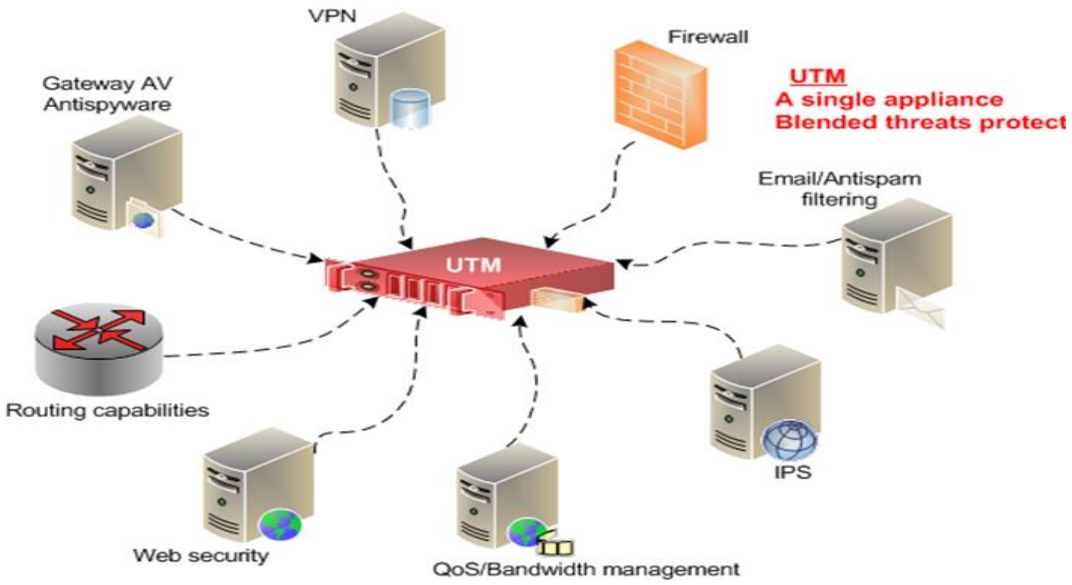
De acordo com Team (2012), essa licença pode ser incluída em produtos proprietários e naqueles com licença privativa do fabricante, como é o caso de produtos da Microsoft e o uso em sistemas operacionais baseados FreeBSD como Mac OS X da Apple Computer.

Isso significa que, com o uso desse firewall, as empresas podem economizar na aquisição de sistema eficaz e barato para sua rede e consequentemente aumentar sua condição financeira.

b) Centralizador de Serviços e Funções

Gerenciador unificado de ameaça (UTM) é uma solução desenvolvida em 2004, pela IDC, com intuito de centralizar vários serviços de segurança em um único dispositivo na rede. Sua administração é feita por meio de interfaces de gerenciamento, em que se pode configurar serviços, recursos e políticas de segurança. Uma vez implantado, esse sistema as organizações não precisaram implantar outros serviços, pois cada usuário possui sua interface e login para gerenciamento desse sistema (FIREWALLS, 2021).

Figura 1 - Topologia de UTM



Fonte: FIREWALLS, 2021

Para RAIDBR (2019), essa solução traz alguns benefícios e vantagem para empresas:

- Ela agrupa diversos recursos para gestão da segurança organizacional em único ativo para facilitar a gestão de analistas e gestores. Nela contém módulos de firewall, Proxy Web, VPN, alta disponibilidade, proteção IDS, Qos e relatórios.
- Oferece uma visão geral da infraestrutura lógica da rede, pois permite verificar acesso de usuários, quais sites são acessados por eles, o tempo de permanência, disponibilidade da internet e estado de links.

- Estabelece diretrizes de acesso no ambiente tecnológico para permitir ou restringir uso de internet na empresa, conforme políticas padrões de segurança.
- Acesso remoto de forma segura com uso de soluções de VPN, que possibilita um acesso seguro, sem a necessidade de expor informações da organização.

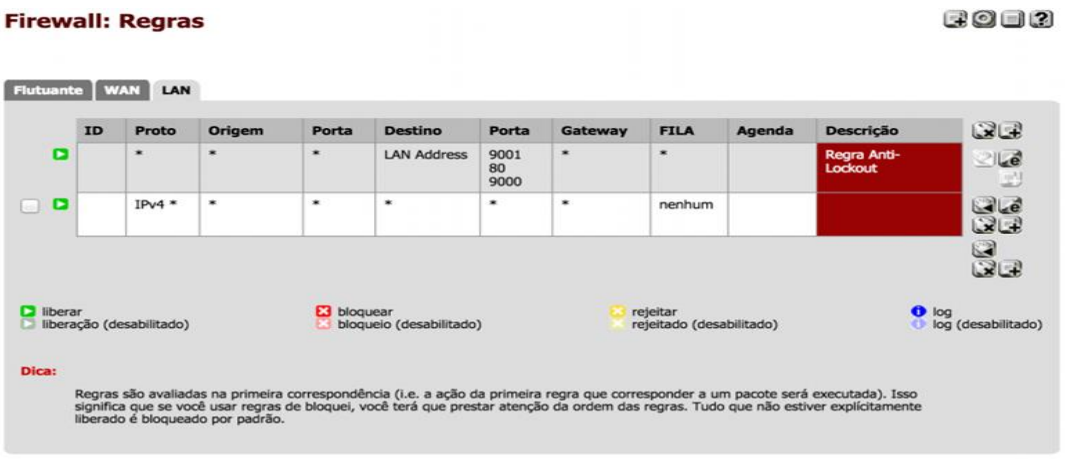
Assim, o PfSense pode reunir diversas soluções em único servidor, evitando que se adquira outras ferramentas para gerenciamento da rede. Além disso, vale destacar a possibilidade de download de aplicações em seu repositório, como cron (gerenciador de processos do sistema), openVPN export client, zabbix entre outros.

c) Firewall do Perímetro de Rede

O firewall do PfSense tem como propósito monitorar o tráfego de dados de uma rede, barrando o fluxo de informações perigosas e protegendo o dispositivo. Em suma, esse sistema realiza tais funções através de políticas de segurança, as quais determinarão se a conexão atende ou não as suas políticas (HENRIQUES, 2020).

Para o autor Henriques (2020), essas políticas de segurança podem ser implementadas no PfSense de acordo com a preferências do usuário, o qual, por exemplo, pode determinar que certo usuário possa fazer download, usar funções online de programas do computador, ou até mesmo acesso a pastas.

Figura 2 - Regra de Firewall do Pfsensel



Fonte: DGTI / IFCE, 2021.

d) Firewall Appliance

Appliance é um dispositivo que tem software integrado ao seu hardware que visa fornecer recursos computacionais para determinada tarefa. Por ter configurações de sistema pré-definidas, seus componentes não podem ser modificados, pois são feitos especialmente para operar naquela arquitetura tanto física como lógica (FERNANDES, 2019).

Como firewall, esse equipamento divide uma rede interna da pública, filtrando os fluxos de dados com base em protocolos, endereço virtual da máquina e portas. Com supervisão de administradores de rede, aquele pode controlar o acesso a serviço e sistemas para os usuários (FERNANDES, 2019).

Para ID Tecnologia (2020), o uso de firewall Appliance em uma pequena e microempresa (PME) são recomendados, pois esses são compactos, baixo consumo de energia e podem ter aplicação gratuita, como Pfsense, embarcada em seu hardware.

Além disso, o autor elenca os principais benefícios do uso desse software nesse dispositivo, como:

- Acesso a relatório completo sobre uso de internet dos usuários, julgar o que pode ou não ser acessado na rede pública.
- Pode acessar a rede interna a qualquer momento e lugar, facilitando, por exemplo, o trabalho home office.
- Balanceamento de carga de links de internet e gerenciar o acesso de usuários a esses links.
- Detectar e bloquear ataques com regras de acesso e impedir, tanto de pacote que entra e sai da rede.
- Instalação de módulos complementares para aumentar números de funções como Proxy Server, Antivírus, IPS/IDS e entre outros.

e) Balanceamento de Carga

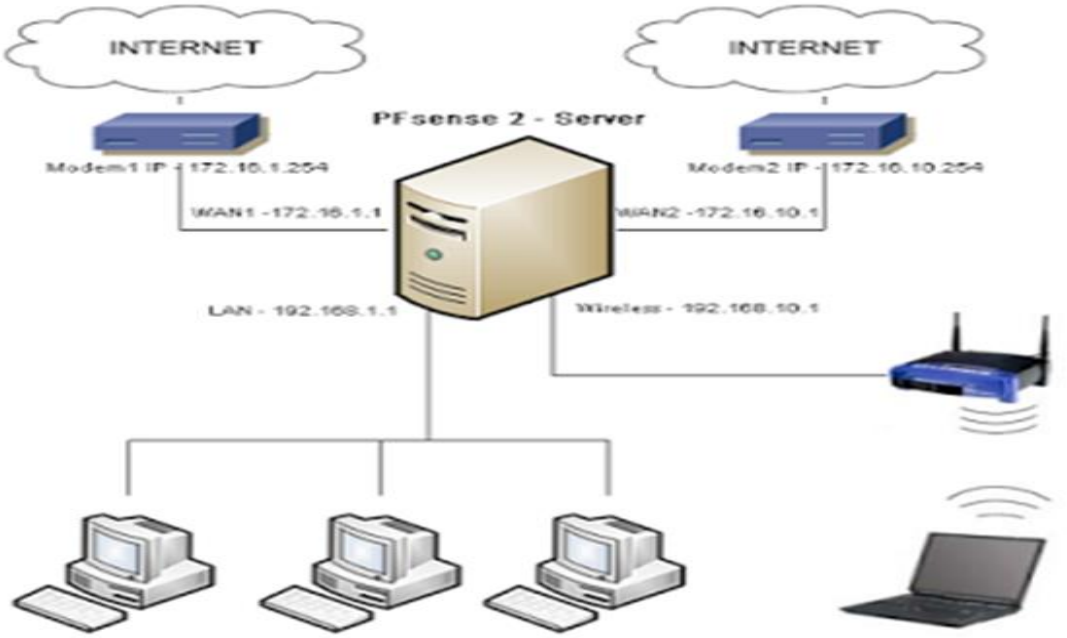
Balanceamento de link ou carga, ou no inglês (failover) é um dispositivo que permite o uso de dois ou mais serviço de internet para equilibrar seu uso conforme a

necessidade do outro, ou seja, quando uma conexão parar a outra assume e estabelece o acesso à internet instantaneamente (FERNANDES, 2019).

Para STRN (2020) essa funcionalidade é dividida em duas no Pfsense: balanceamento de carga para gateway e o balanceamento de carga para servidor. O primeiro divide o fluxo de dados da internet por intermédio de interface WAN. Já o segundo permite que o fluxo de dados da internet seja distribuído entre vários servidores da Web e servidores SMTP, ainda que qualquer use TCP ou DNS.

O autor STRN (2020) ainda cita um recurso chamado de multi-WAN do PfSense que permite o firewall utilizar várias interfaces WAN (10 a 12 interface). Com essa funcionalidade, trata todas as interfaces com uma única, idêntica na GUI.

Figura 3 - Topologia de rede com balanceamento de carga



Fonte: Jonas, 2015.

Além disso, essa funcionalidade pode ser usada como mecanismo de redundância na rede. Quando dois links de internet são inseridos no servidor PfSense, o administrador poderá definir qual interface será primária (usada para provê acesso ao mundo externo) e qual ficará ociosa para substituir aquela quando houver queda no link.

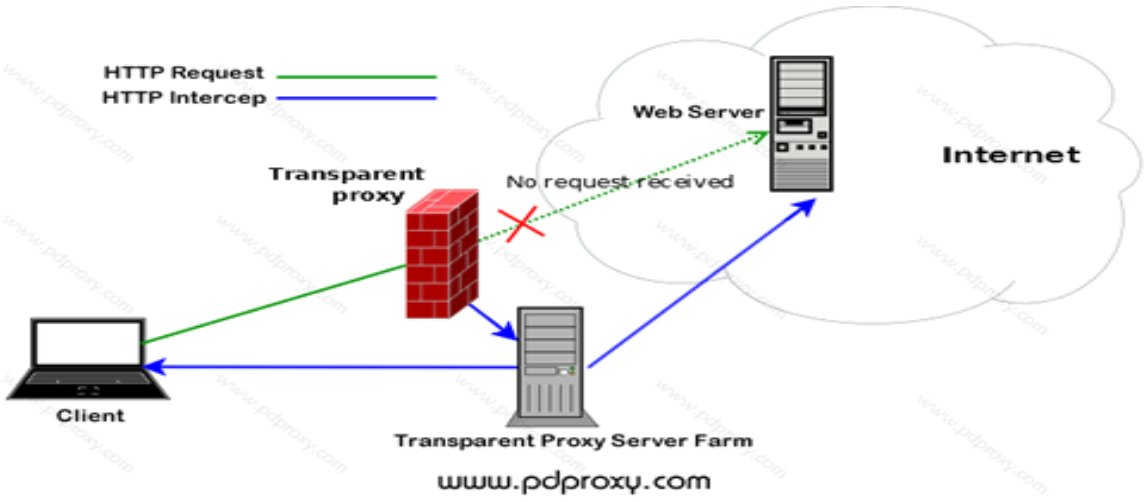
f) Servidor Proxy

Um servidor proxy é aquele que intermedia requisições de um cliente entre servidores web hospedados na internet. Ele pode estabelecer, dependendo da política empregada na empresa, regras para um usuário ou a todos dentro da rede (FERNANDES, 2019).

Além disso, aquele ajuda no processamento rápido de páginas da Internet, guardando consigo uma espécie de cópia da página web (cache), que, quando requisitada novamente, o servidor verificará se esta consta ou não em seu banco de dados. Uma vez contida lá, ela é carregada de maneira rápida, como se não tivesse feito uma requisição novamente.

No contexto da ferramenta estudada, esse servidor pode ser implementado de várias maneiras: com servidor SquidGuard (um software usado para controlar tráfego de dados no meio externo por regras e filtros) ou por meio de proxy transparente (comumente usados para esconder o tratamento das informações enviadas ao servidor web na internet).

Figura 4 - Funcionamento de Proxy Transparente



Fonte: It9, 2016.

g) Capitive Portal

O Captive Portal é um software do PfSense que força usuários de uma interface a se autenticarem antes de acessar a Internet. Normalmente ele apresenta um portal

que possui login e senha para ser autenticado, assim como voucher ou um simples botão na página (NETGATE, 2020).

Esse recurso é comumente usado em hotéis, restaurantes, hospitais, aeroportos, ambientes corporativos e domésticos como casa, por exemplo. Ademais, ele é muito usado em redes sem fio, ou para autenticação de usuários internos que precisam de acesso à internet (NETGATE, 2020).

h) Interface Gráfica

Ele possui em sua página inicial de gerenciamento web, uma interface que contém dados, gráficos, a fim de auxiliar no monitoramento de redes, interface e serviços ativos no Pfsense. Além do mais, pode-se personalizar os gráficos utilizando aplicações disponíveis no repositório do sistema operacional como telegraf e grafana.

Figura 5 - Interface inicial do Pfsense personalizada

Fonte: Bergeron, 2018

i) Servidor DHCP

Protocolo de configuração dinâmica de hosts (DHCP) é um servidor que fornece configurações para hosts da internet. Em sua estrutura tem-se um protocolo que fornece configurações específicas do servidor e um mecanismo que faz a alocação de endereços aos hosts conectados na rede (RFC 2131, 1997).

O DHCP funciona como cliente-servidor, no qual é configurado com parâmetro da rede (IP, DNS, sub-rede, gateway) e quando um cliente solicita conexão a esse servidor, ele recebe esses dados automaticamente, sem a necessidade de configurá-lo manualmente (RFC 2131, 1997).

O servidor DHCP do Pfsense permite que administradores de rede criam intervalos de endereço IP, configurar DNS e domínios automaticamente na concessão dos endereços virtuais, criar lista de usuários que possam ou não solicitar esse serviço, além do mais, pode-se isolar um grupo de endereço dos demais com uso de IP estáticos (muito usado para separar servidores e a rede local como todas).

j) Servidor VPN

OpenVPN é um aplicativo de software que pode criar um túnel na internet com usuários de um lado e o servidor na outra extremidade. Essa ferramenta é open source, pois sua estrutura pode ser alterada por qualquer pessoa ou grupo, a exemplo da comunidade OpenVPN center (BOZOVIC, 2019).

Essa aplicação é multiplataforma, suporta clientes Windows, Mac OS X, sistemas baseados BSD, Linux Solaris e Windows Mobile. Para Android, essa ferramenta é gratuita, não requer qualquer permissão avançada do sistema operacional (NETGATE, 2021).

WireGuard é um protocolo VPN com código aberto que permite simplificar os processos de segurança de dados. Essa solução possui métodos mais rápidos e simples do que é usado nos protocolos do OpenVPN e IKEv2, mais usados atualmente (MILIN-ASHMORE, 2021).

Para Netgate (2021), os clientes deste protocolo têm a possibilidade de usar VPN em vários sistemas operacionais, entre eles estão Windows, Mac OS X, FreeBSD, Linux, Android, iOS e entre outros. Além disso, algumas versões requerem instalação de software cliente de outros, como é o caso do Linux.

IPsec é um protocolo que está na camada 3 (Rede) do modelo TCP/IP que permite acesso remoto a uma rede interna por meio de VPN. Ele é comumente usado para comunicações de máquina remota e seu tráfego de dados é enviado pela rede pública, criptografado entre servidor e host (NETO, 2020).

Conforme Netgate (2020), embora as aplicações nativas deste protocolo não suportem algumas configurações, ele está disponível para Windows, Mac OS X, BSD, Linux e outras plataformas. Na versão Mac OS X, por exemplo, estão incluídos IKEv2 e Cisco IPsec.

k) DNS Dinâmico

O DNS Dinâmico é um serviço que permite atribuir nomes a dispositivos de rede com endereços aleatórios. Ao ser comparado, por exemplo, com o estático, esse atualiza as informações internamente, podendo conectar e mudar de endereço IP de uma máquina sem que usuários percebam essa transação (KAGUTECH, 2021).

O Cliente DNS dinâmico integrado ao Pfsense associa um endereço IP a uma determinada interface WAN, que permite o uso de serviço de acesso remoto a usuários da rede. Ele pode ser também configurado para mais de 20 provedores de DNS dinâmicos, podendo ser aplicado a provedores customizados e registrar um endereço real em ambientes que o firewall recebeu um IP privado do seu provedor de acesso (NETGATE, 2020).

l) Serviço NAT

Network Address Translation (NAT) é uma solução desenvolvida para lidar com a escassez de endereços IPv4 no mundo. Ela permite que usuário tenha uma quantidade suficiente de endereço para uso em uma rede interna, separando o tráfego em rede grande para rede interna e pequenas para externa (FOROUZAN, 2010).

No geral, ela permite que computadores sejam conectados à internet por meio de um endereço público, na versão IPV4. No contexto do Pfsense, ele pode ser implementado com uso simples ou em configurações mais avançadas e complexas (NETGATE, 2020).

m) Servidor PPPoE

PPPoE ou Point-to-Point Protocol over Ethernet é um protocolo que interliga vários usuários a uma interface em uma rede LAN com uso de link DSL. Ele é usado

para identificar e controlar ações de usuários autenticados nesse serviço. O controle é baseado no monitoramento de tráfego da banda e na identificação do modem (endereço MAC), os quais possibilitam criar regras de acesso com mais rapidez (CANALTECH, 2017).

O Pfsense pode atuar como um servidor PPPoE como ponto central de controle, aceitando, autenticando usuários a uma interface local do servidor. Ele permite que administradores forcem a autenticação de usuários para obter acesso a internet ou controlar logins destes (NETGATE, 2020).

6 IMPLEMENTAÇÃO

6.1 Materiais Envolvidos

6.1.1 Softwares

Para o desenvolvimento deste trabalho foi necessário o uso de ferramentas específicas para rede de computadores, como:

- VirtualBox versão 6.1
- Pfsense na versão 2.5.3 CE 64Bits
- OpenVPN
- Samba
- MySQL
- Windows e Linux

6.1.2 Hardwares

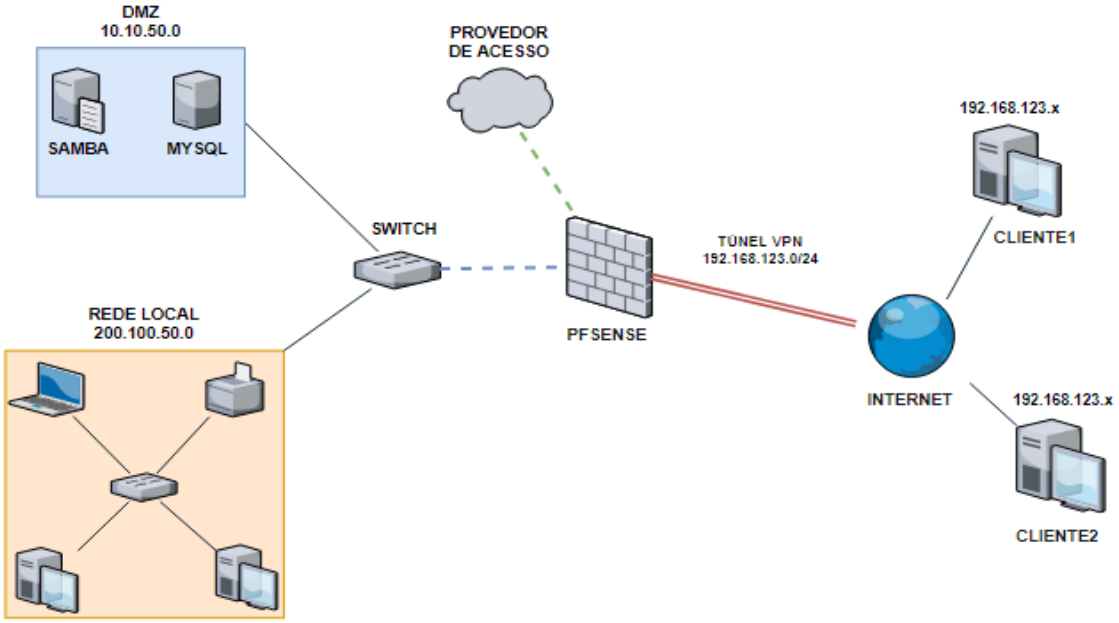
Para a instalação das aplicações selecionada anteriormente, foi usado os seguintes equipamentos:

- Notebook HP
- Roteador GPON
- Computador Desktop
- Roteador Domestico TP-Link 150
- Smartphone Android (para teste em versão mobile)

6.2 Topologia de Rede

Inicialmente optou-se pela topologia estrela, pois mostrou-se ser mais eficiente em organizar fisicamente os periféricos e possuir critério de confiabilidade, segurança e desempenho bem aceito pela área de rede. Assim, a figura 6 mostra como sua estrutura foi desenvolvida e organizada.

Figura 6 – Topologia para implementação do Pfsense



Fonte: Autoria Própria, 2021

O provedor de acesso é a rede que intermedia a comunicação com a internet, fornecendo esse serviço por meio de cabeamento, satélite ou sem fio. Portanto, configurou-se a placa 1 do firewall com endereço do servidor DHCP. Ademais, identificado por Firewall VPN, encontra-se o Pfsense, que é uma máquina virtualizada com uma imagem ISO do sistema instalado no Virtualbox. Sua função é criar um canal de conexão entre os servidores internos e clientes na internet, bem como controlá-lo através de regras.

Na DMZ foram criados dois servidores para fazer testes da conexão entre as duas extremidades e isolar o acesso de outros usuários a esses serviços. O MySQL é um servidor de armazenamento de dados em grande escala (banco de dados) e o samba que oferece compartilhamento de arquivo, impressora, computadores e etc.

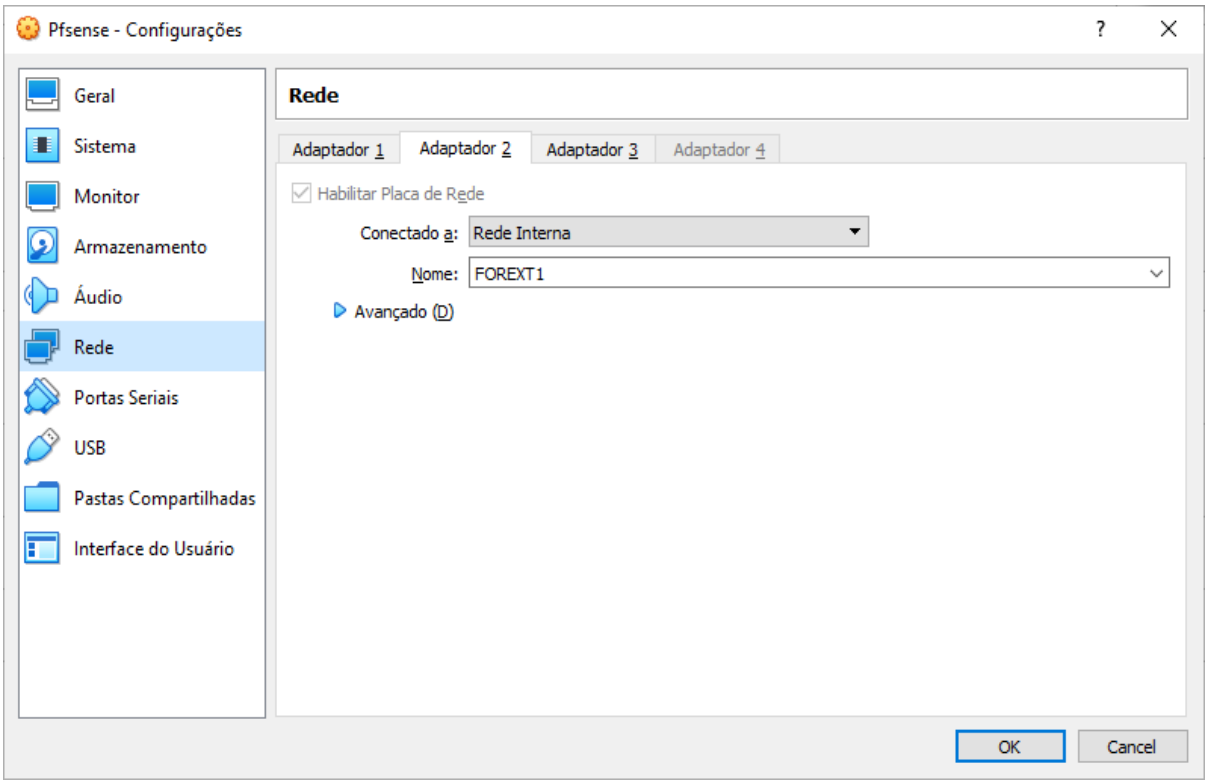
A LAN é uma rede que contém toda infraestrutura interna da topologia. Ela possui os ativos da rede como computadores, impressoras, servidores de uso interno e outros. Enquanto o Switch tem a função de interligar as redes local e a DMZ ao firewall. Dessa forma, conectou-se, por meio virtual VLAN do Virtualbox, firewall, rede interna e a rede desmilitarizada.

Por fim, o túnel de acesso VPN é responsável por prover acesso aos usuários autenticados nesse serviço acessem recursos da rede pela internet de forma segura.

6.3 Configurações do VirtualBox

Nessa etapa foi aplicado as configurações de rede nas maquinas virtuais para conexão da rede.

Figura 7 - Configurações de Rede no VirtualBox



Fonte: Autoria Própria, 2021

Na máquina Pfsense foi configurado duas interfaces: modo bridge e a modo interno. A primeira é usada para simulações de rede e execução de servidores em um modo convidado. Quando ativada, a aplicação conecta-se às placas de rede (wireless, ethernet, bluetooth) do cliente e há troca de pacotes entre dois, assim, simulando um equipamento físico conectado na placa. Já o segundo modo é usado para isolar um conjunto de máquinas virtuais do meio externo, deixando-as visível somente aquelas conectadas a sua rede.

Desse modo, usamos a rede bridge para se conectar à internet, recebendo um endereço do servidor DHCP do modem e a interface interna para isolar a Rede Local e hospedar os servidores de teste.

6.4 Configuração de Rede

Na configuração de rede do sistema criou-se quatro interfaces para conexão entre servidores e os clientes.

- WAN (192.168.1.0 / 24) – Rede Externa
- LAN (200.100.50.0 / 24) – Rede Interna
- DMZ (10.10.50.0 / 24) – Rede dos Servidores
- TNEL_VPN (192.168.123.0 / 24) – Rede do TúnelVPN

Ainda, foram reservados endereços IP para os servidores:

- Pfsense (200.100.50.10)
- Samba (10.10.50.7)
- MySQL (10.10.50.5)

Já no servidor DHCP criou-se um escopo de intervalo com endereços para computadores conectados na LAN:

- 200.100.50.30 até 200.100.50.60

Figura 8 - Terminal de linha de comando do Pfsense

Fonte: Autoria Própria, 2021

6.5 Samba

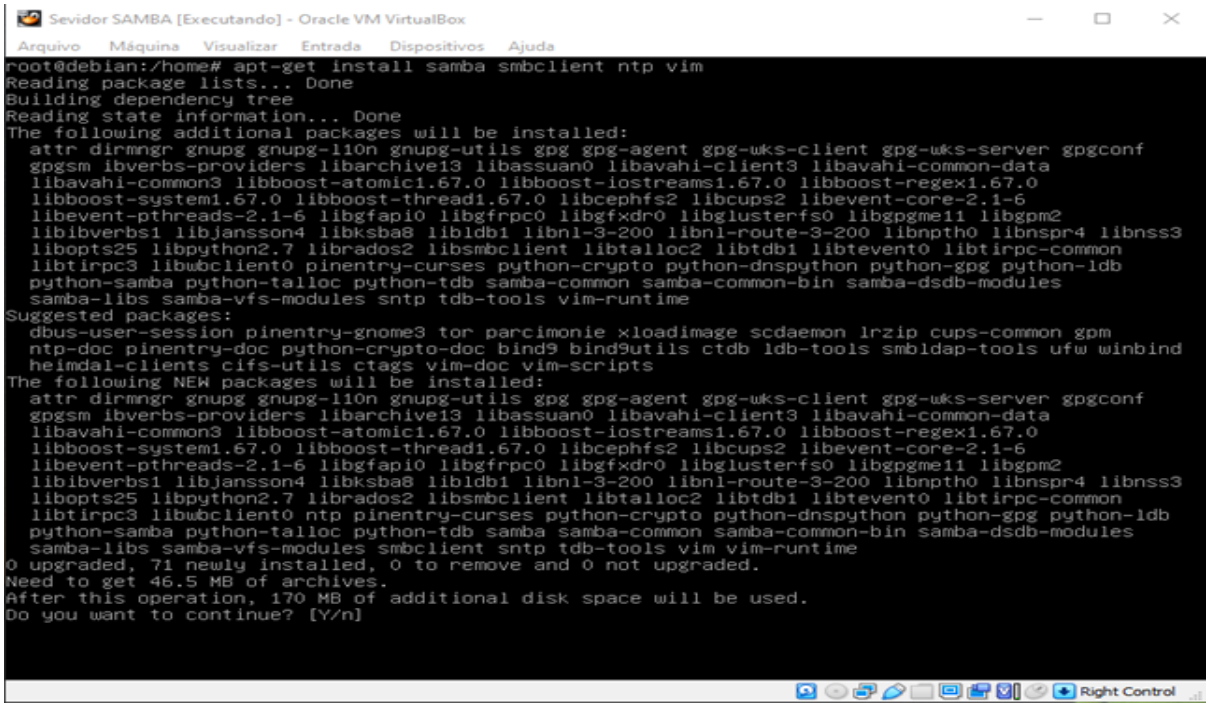
6.5.1 Instalação do Samba

Para exemplificar uma rede com compartilhamento de arquivos usamos o servidor Samba. Esse programa permite compartilhar pastas, arquivos, impressoras e usuários de computadores, o que facilita no dia a dia dos funcionários de uma empresa.

Para sua instalação foram selecionados pacotes disponíveis no repositório do Debian: samba, smbclient e o vim.

Ao iniciar a máquina foi necessário atualizar os pacotes de repositório do sistema utilizando o comando "apt-get install update". Depois digitou-se o comando "apt-get install samba smbclient vim". E ao apertar a tecla enter, foi confirmada com a letra “Y - Yes” para prosseguir o processo.

Figura 9 - Tela de Instalação do Samba no Debian



Fonte: Autoria Própria, 2021

Finalizado o processo de instalação do servidor, entrou-se na pasta de configuração do samba e foi inserido determinados parâmetros para o bom funcionamento desse servidor.

6.5.2 Configuração do Samba

Assim como o servidor SSH, FTP e o DNS, o samba possui um arquivo de configuração, o qual se pode fazer mudanças no funcionamento. Assim, entrou-se no diretório que se encontrar conteúdo da aplicação e editou-se o “smb.conf” com parâmetros para compartilhamento de pasta e modo de acesso a estas.

6.5.3 Criação de pasta compartilhada

O compartilhamento de pastas é essencial para armazenar e acessar conteúdos de outro computador. Para acessar e armazenar arquivos no servidor SAMBA foi necessário a criação de pastas. Em primeiro lugar, criou-se três pastas com os seguintes nomes: pasta1, pasta2 e pasta3. E em seguida, criadas as contas de usuário do sistema, divididas conforme seu setor e ao final foi atribuído permissões de acesso à estas para garantir sua segurança.

Esses diretórios foram usados para testar a eficiência da conexão VPN, por isso a criação deles bem como sua configuração de acesso e usuários.

6.5.4 Autorização de acesso a diretórios

O chmod é um comando nativo do UNIX que altera as permissões de arquivos e pastas, sendo elas ordenadas em número ou letras. No Linux, cada arquivo possui um campo de permissão a qual atribui-se um dono, grupo e outros usuários. Nesse sentido, foram criadas as permissões para pastas de compartilhamento, que receberam os seguintes atributos:

*# chmod 755 /home/pasta**

Essa numeração possui nomenclaturas para um bom entendimento, as quais se atribui os seguintes nomes:

- Permissão de leitura, gravação e execução;
- Somente leitura e execução.

O primeiro faz referência ao número 7, o qual permite qualquer modificação na pasta pelo administrador do sistema. Com referência ao número 5, o segundo concede somente permissões aos usuários em grupo e convidados. A combinação desse número permite que o sistema faça modificação no acesso, na leitura e nas execuções diretório e arquivos.

6.6 Mysql

Nessa etapa foi criado um banco de dados como uso de pacotes disponibilizados no repositório Debian. Para isso foi instalado mysql-server com o comando “apt-get install mysql-server” e em seguida feita suas configurações iniciais tais como definição de senha, apagamento de usuários convidados e outras.

Para criar tabelas nesse banco de dados foi necessário a criação de uma database com o nome “Usuários”, que foi responsável pelo armazenamento das informações, por exemplo, de um departamento de uma empresa. Em seguida foi criado um usuário para acesso remoto com os comandos “CREATE USER raiander@200.100.50.10 TO IDENTIFIED BY ‘12345678’; “ e “GRANT ALL Usuários. * TO raiander@200.100.50.10; “. O primeiro comando foi responsável por criar o usuário e identificar o endereço IP do cliente e sua senha de acesso, enquanto o segundo cedeu acesso à base de dados.

Por fim, para exemplificar o acesso de dados neste banco de dados, foi importada uma base de dados com lista de servidores do governo de São Paulo, a qual tem acesso e o direito de usa-la livre e gratuito. Ela foi responsável por alimentar a base com dados como nomes, números, datas e outros para posteriormente ser consultado com comando da linguagem SQL.

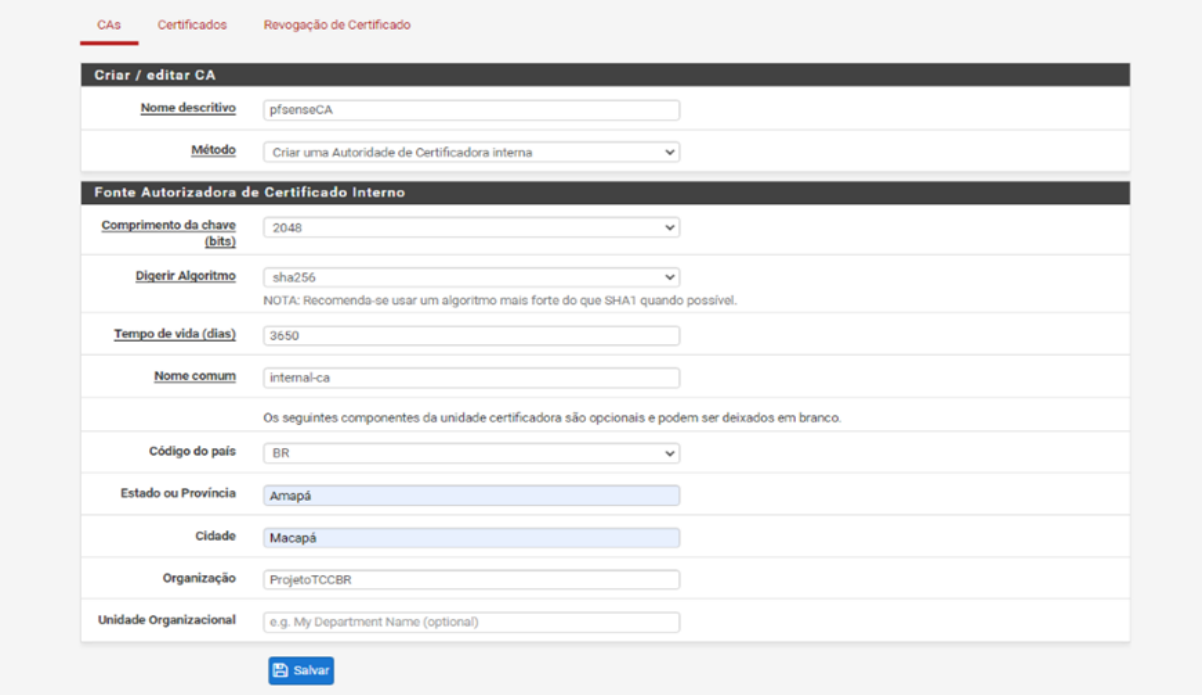
6.7 Configuração do Pfsense

6.7.1 Criação do Certificado HTTPS

O Certificado de Autoridade é um documento digital emitido por uma organização para vincular determinado site, servidor ou serviço a esse certificado.

Esse documento permite que seja conhecida a origem e a credibilidade do site. Desse modo, foi criado o certificado para servidor da seguinte forma: entrou-se na opção Sistema - Gerenciador de Certificados, opção CAs e em seguida Adicionar, no qual foi preenchido os campos em branco, como mostra a figura 10.

Figura 10 - Criação de certificado para autenticação do servidor



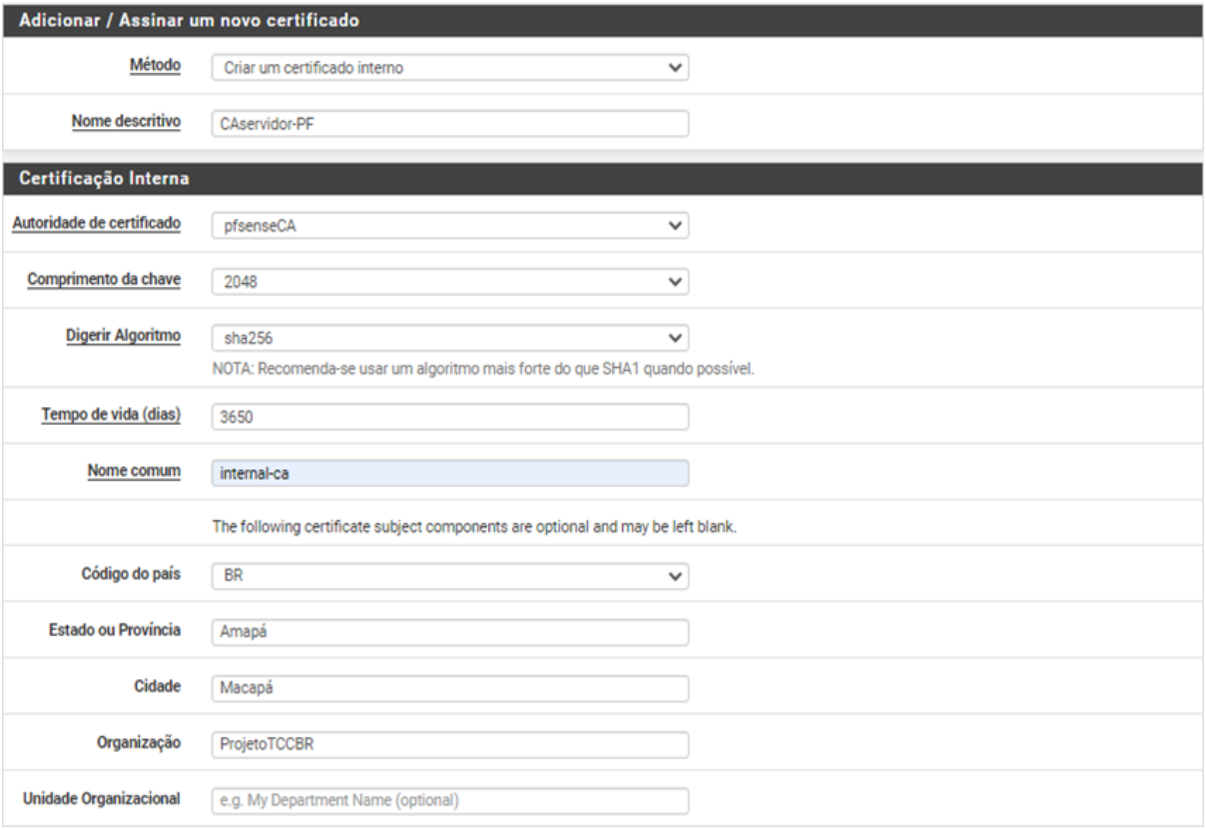
Fonte: Autoria Própria, 2021

No método utiliza-se autoridade interna para criar dados vinculados ao servidor; nome comum é o nome dado a servidor no certificado digital; a organização é o nome da empresa que é responsável pelos serviços. Após o preenchimento dos dados foi alterado o método de criptografía para algoritmo SHA 256, que é mais adequado para serviços como VPN e SSH.

No gerenciador de certificado seleciona-se a opção Certificado. Nessa etapa foi criado um certificado para o servidor. Ele vincula endereço ou hostname do servidor com um certificado para acesso interno.

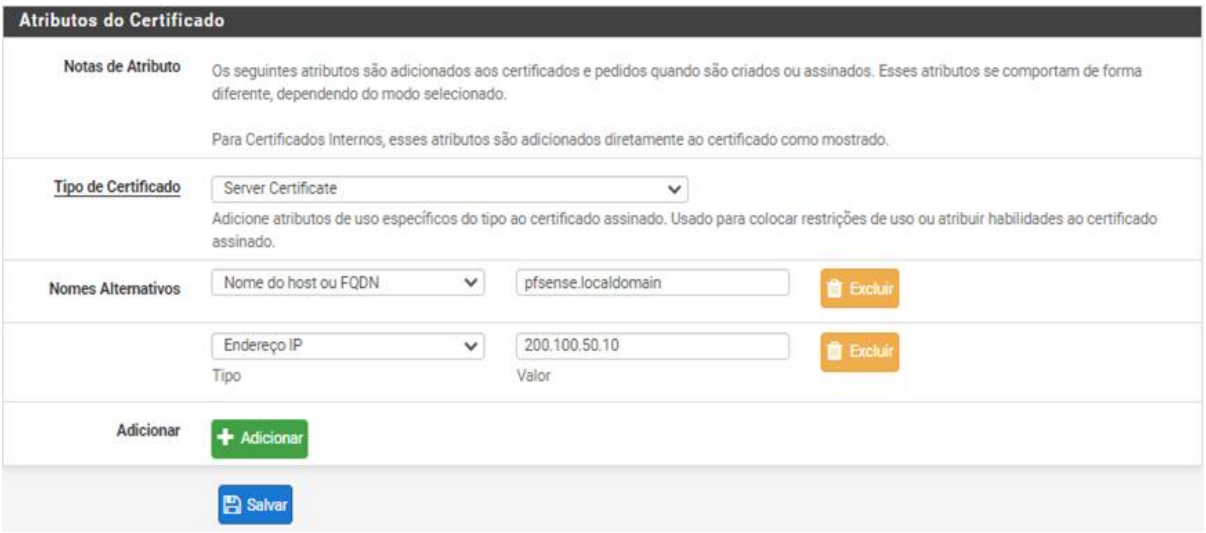
Primeiramente foi marcado a opção "criar um certificado interno" e em seguida o nome para o certificado. Na opção nome comum foi inserido o nome do certificado de uso da internet. Na opção Atributo do Certificado alterou-se para “Server Certificante" e no nome alternativo inserimos endereço do serviço e nome da máquina.

Figura 11 - Criação de Certificado para Servidor



Fonte: Autoria Própria, 2021

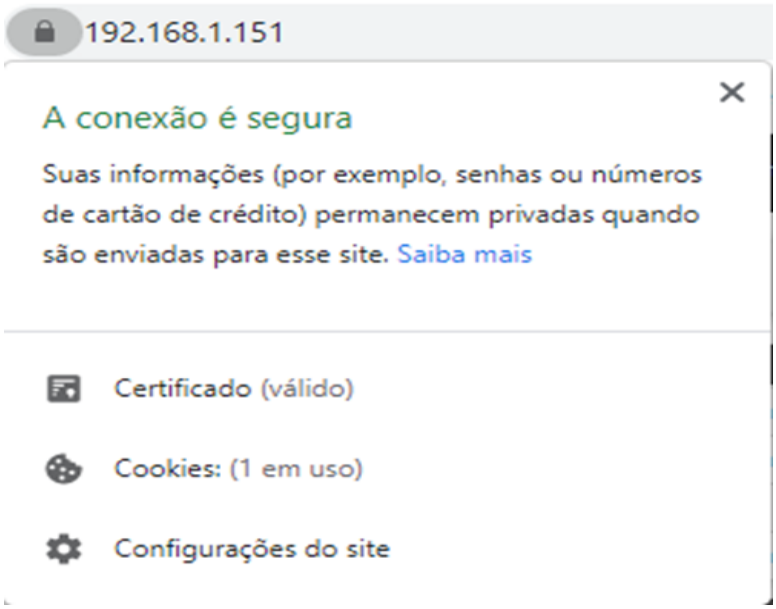
Figura 12 - Configuração atributo ao certificado



Fonte: Autoria Própria, 2021

Por fim, a opção “Sistema - Avançado” foi marcada a opção HTTPS, a qual permitiu que alterasse o certificado padrão do servidor para “PfsenseCA”, criado anteriormente.

Figura 13 – Tela Inicial do Pfsense com HTTPS



Fonte: Autoria Própria, 2021

Essa configuração de certificado é essencial para conexão de VPN, pois essa tecnologia utiliza-se principalmente de criptografia de ponta para provê um canal seguro entre o cliente e o servidor por meio de um canal inseguro como a internet e a decodificação desse mercanismo na aplicação cliente.

6.7.2 Instalação do OpenVPN

Após a configuração do Pfsense, foi instalado a aplicação OpenVPN, que funcionou como forma de prover conexão entre servidores e os clientes. Dessa forma entrou-se na opção Sistema – Gerenciamento de Pacote – Pacotes disponíveis e instalou-se a extensão “openvpn-client-export”, que fica responsável por ceder arquivos de configuração aos clientes.

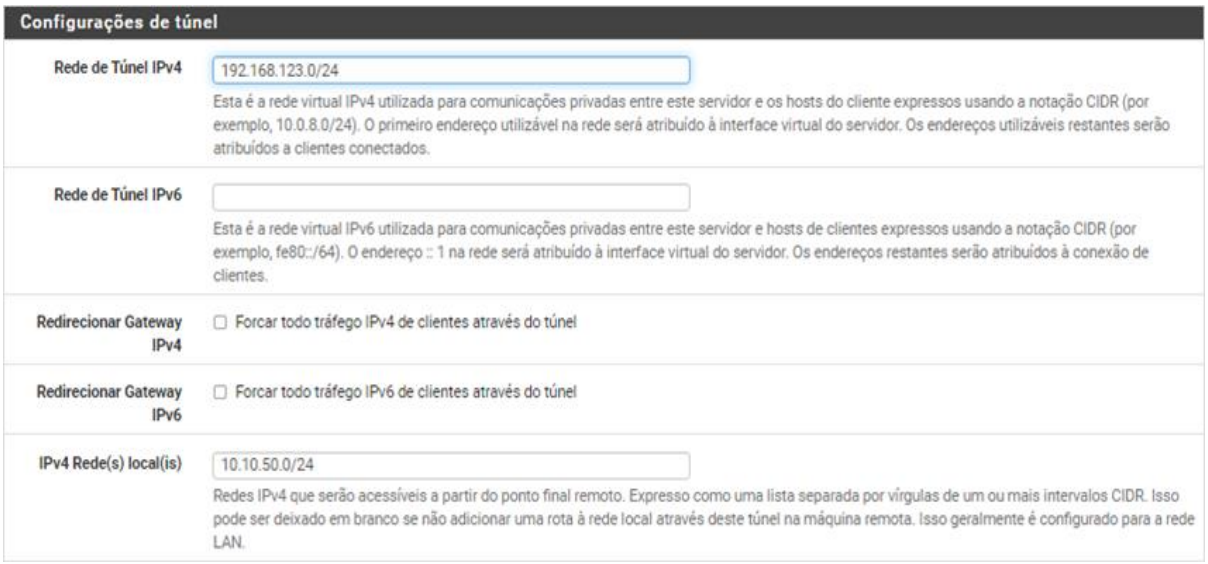
6.7.3 Configuração do Servidor VPN

O modo Wizard (modo assistente) do OpenVPN é a forma mais simples de configurar VPN para acesso remoto no PfSense. Assim, foi escolhido o modo acesso de usuário, o qual permite que usuário acesse o servidor e recursos espalhados pela rede. Em seguida, configurou-se o modo de acesso atribuindo parâmetros, como

mostrado na imagem abaixo, os quais deram destaque ao campo de protocolo e à porta.

Nos parâmetros de configuração do túnel, foram atribuídos endereços IP nas opções: rede de Túnel e Rede local. A rede de tunelamento foi responsável pela conexão entre o servidor e os clientes. Enquanto a rede local atribui-se o IP interno.

Figura 14 - Definição de endereço do Túnel VPN



Fonte: Autoria Própria, 2021

Por fim, foi salvo as configurações e dado o prosseguimento para a criação de regras de tráfego.

Na opção Tráfego de Clientes para Servidor foi marcado a caixa de regra de firewall, o qual permite que clientes externos possam conectar no servidor. Ademais, atribui-se a regra da opção Tráfego de Clientes por VPN, que permite o acesso dos clientes pelo túnel da rede privada.

Para conectar-se a uma VPN é preciso ter autorização de acesso do servidor e obter um certificado emitido pelo Pfsense. Desse modo, foram criadas duas contas para teste, sendo elas identificadas como cliente 01 e cliente 02.

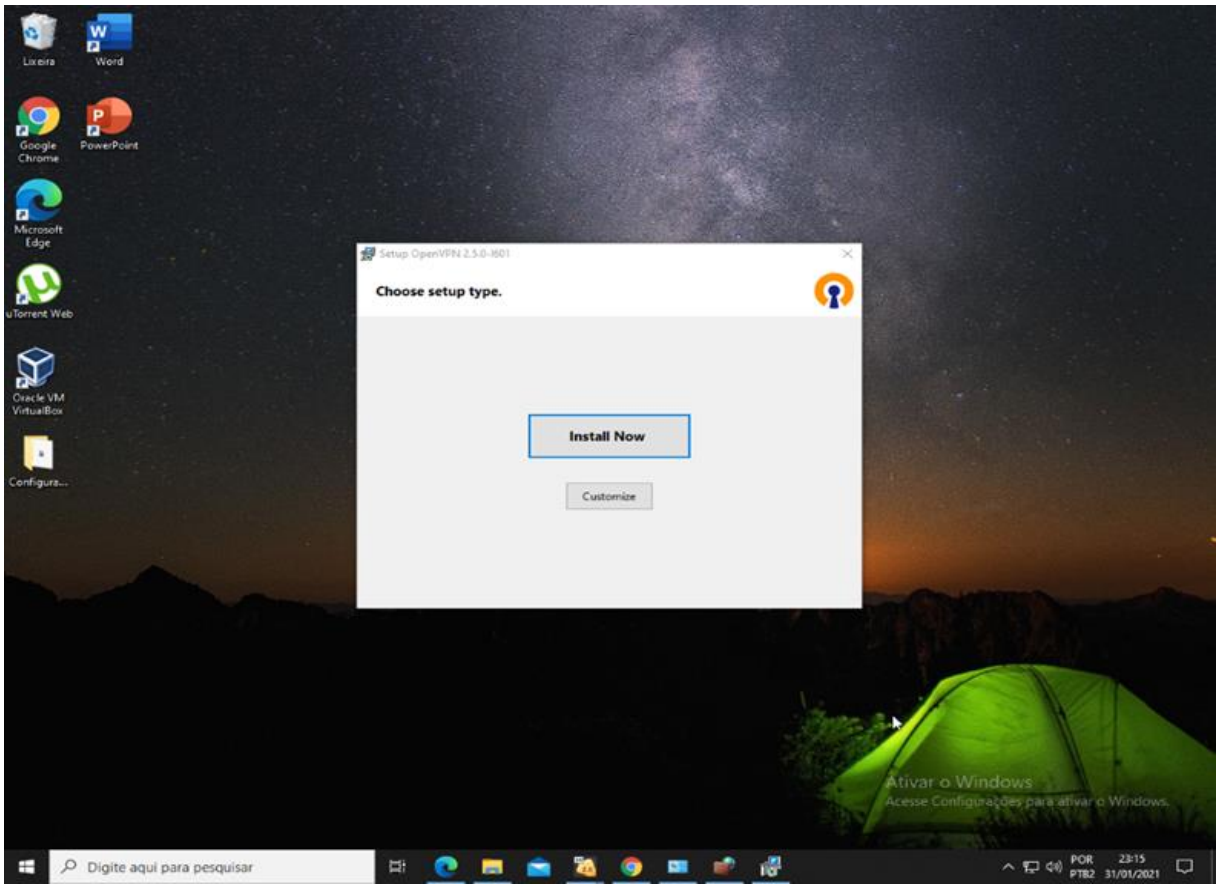
Ao criar contas de usuários entrou-se na opção Sistema - Gerenciamento de Usuários e adicionou novo. Atribui-se o nome do cliente e a senha nos campos nome e senha/repetir a senha. Em seguida, marcou a opção “criar certificado para usuário", atribuiu um nome ao certificado do usuário e salvou.

6.7.4 Exportação de configuração e Autenticação de usuários

Nessa etapa extraiu o arquivo de configuração do OpenVPN. Assim, entrou-se na opção "Serviços - OpenVPN - Client Export” e selecionou a configuração conforme o sistema operacional usado para essa implementação, no caso Windows 10.

Após isso, foi instalado a aplicação disponibilizada pelo servidor no sistema operacional com as configurações sugeridas pelo instalador.

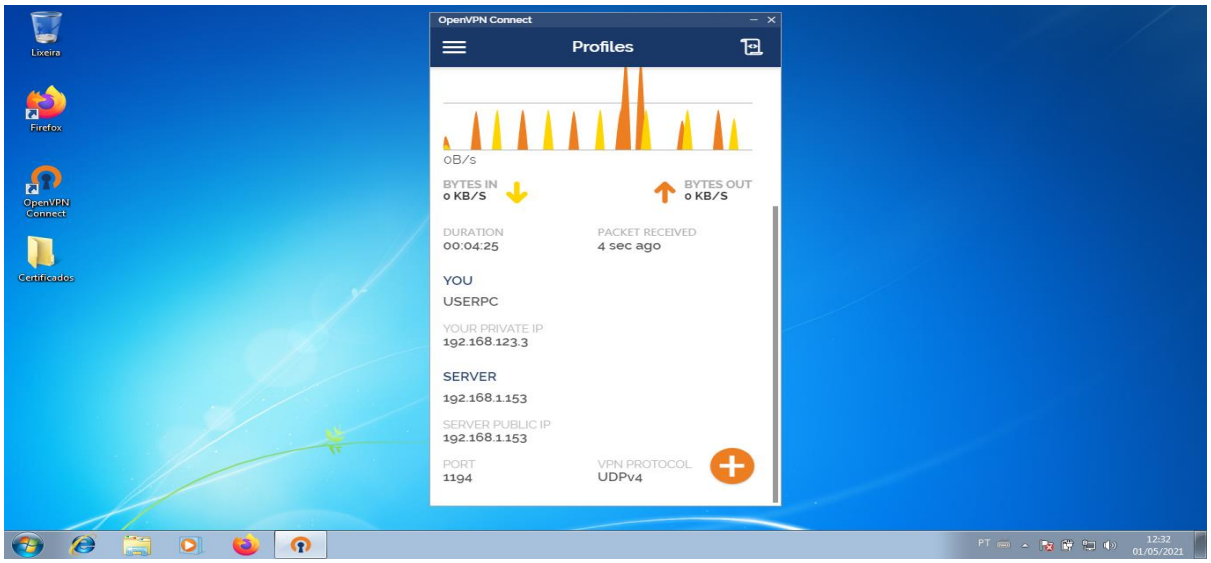
Figura 15 - Instalação do OpenVPN no Windows



Fonte: Autoria Própria, 2021

Terminada a instalação, foi importado o arquivo do ambiente de cliente do servidor, o qual possui a extensão OVPN, configurações do cliente e chave usada para comunicação com o Pfsense. Ao final, foi adicionado nome de usuários e a senha de acesso para autenticação no servidor e realizada a conexão com sucesso.

Figura 16 - Conexão VPN no cliente 02



Fonte: Autoria Própria, 2021

7 TESTE DE USUABILIDADE

Para demonstrar o funcionamento do PfSense com VPN, foi necessário uso de ferramentas comumente utilizadas nas empresas. Entre elas estão servidores MySQL e Samba que possuem papel importante dentro das organizações.

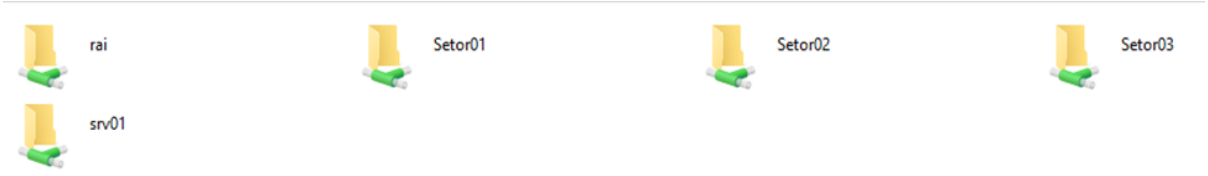
O samba foi usado para compartilhar pastas entre setores e pessoas e impressoras entre grupos do mesmo setor, enquanto o MySQL teve como principal propósito criar conjunto de tabelas relacionais para armazenamento de dados pessoais, informações de clientes entre outros.

7.1 Uso do samba

Para acessar o primeiro serviço do samba, foi usado duas ferramentas que suportam o uso do protocolo SMB: Windows Explorer, aplicação SMB no Android e no Linux.

Primeiramente, no gerenciador de arquivo foi preenchida a barra de pesquisa com endereço IP do servidor "smb:// 200.100.50.8", antecedido com o protocolo SMB. Após isso, foi perguntado o login de acesso ao sistema, o qual foi configurado para receber a permissão para usuários convidados. Em seguida, o servidor autenticou as informações passadas anteriormente, exibindo as pastas autorizadas para esse usuário.

Figura 17 - Pasta do Diretório Samba no Windows.



Fonte: Autoria Própria, 2021

Na aplicação foi criado perfil com dados (domínio, usuários, senha e o endereço IP do servidor samba). Em seguida foi mostrada a tela de autenticação de usuários e entrou-se nas pastas permitidas e adicionou arquivo e documentos. Com esse modo, o usuário pode usar o compartilhamento de pastas sem a necessidade de aplicativos

específicos, facilitando o trabalho para aqueles que não têm conhecimento básico na informática e que necessite do acesso direto no celular.

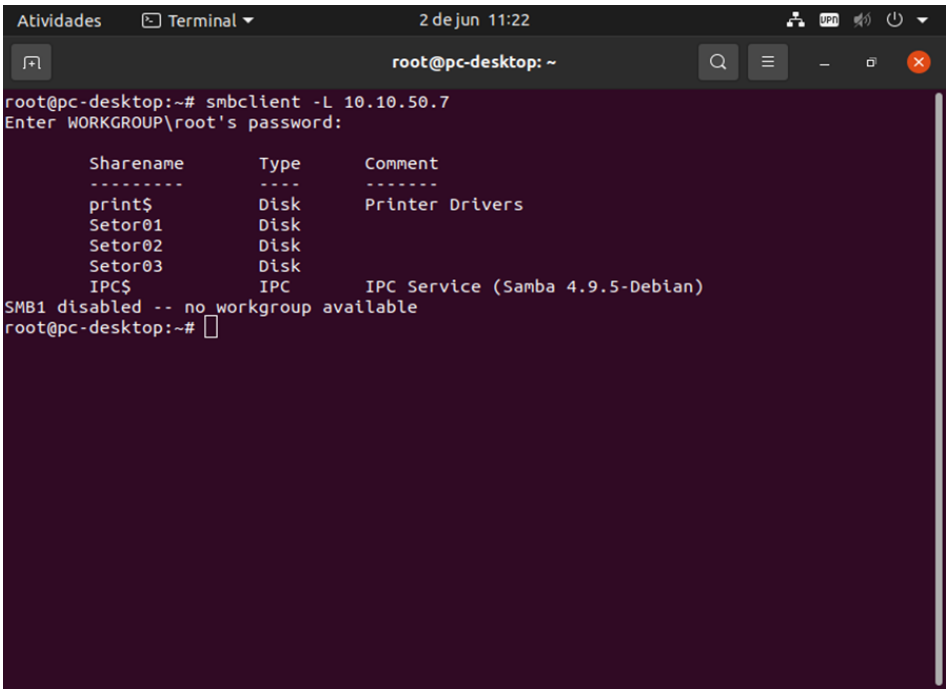
Figura 18 - Acesso remoto de pasta no Android

Fonte: Autoria Própria, 2021

Uma vez logado no sistema, foi possível modificar os conteúdos da pasta e inserir arquivos no diretório, usar uma impressora, além disso, pode-se compartilhar documentos como pdf, xlsx, docx, essenciais para um escritório, por exemplo. Dessa forma esses dados são armazenados no sistema interno da empresa, sem a necessidade de soluções de nuvem.

No sistema operacional linux, foi usado a versão de teste do samba. Esse programa foi iniciado a partir do terminal de comando, vindo a ser executado posteriormente no gerenciador de arquivo do sistema. Ao abrir a tela do terminal, foi inserido o comando “smbclient –L 10.10.50.7”, o qual permite verificar quais serviço estão disponíveis nesse endereço e listar as pastas compartilhadas por este servidor. Após isso, foi possível verificar o bom funcionamento da aplicação e as pastas disponíveis para usuários.

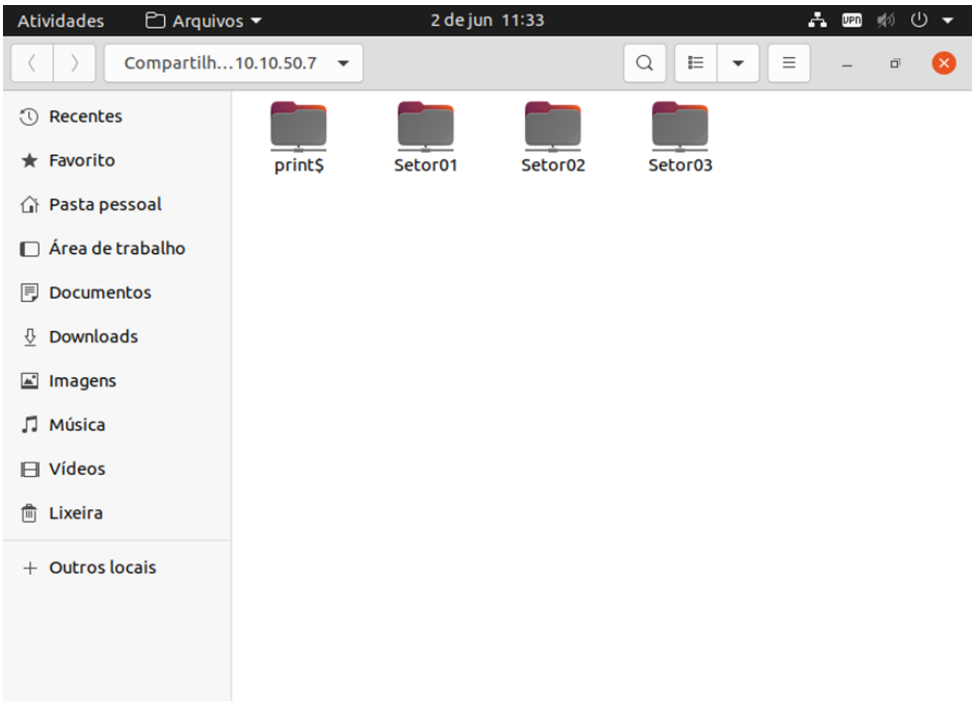
Figura 19 - Teste do servidor samba no linux.



Fonte: Autoria Própria, 2021

Ao final foi aberta as pastas compartilhadas no gerenciador de arquivo ubuntu, o qual permite usar protocolo SMB, tanto para redes windows quanto para servidor como samba.

Figura 20 - Pasta compartilhada abertas no Linux



Fonte: Autoria Própria, 2021

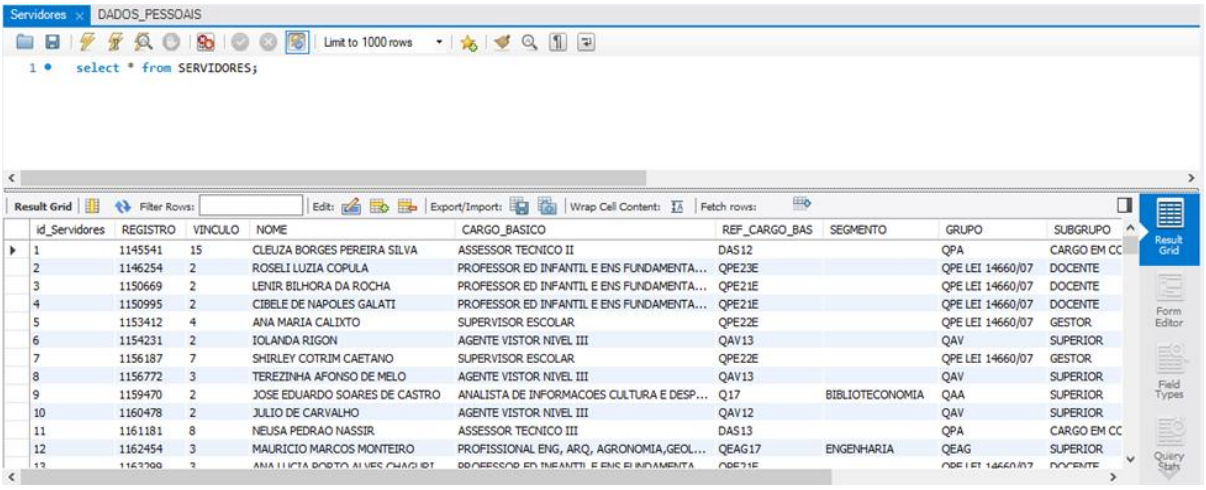
7.2 Uso do mysql

Como o MySQL tem suas aplicações especificadas, foi usado o software Workbench, que permite acessar, manipular e administrar uma base de dados com interface gráfica e a linguagem SQL.

Feitas as configurações de usuários e base de dados, foi criada uma regra no firewall que permite acessar o servidor no endereço “10.10.50.8” e a porta “3309”. Em seguida foi concedida a permissão de acesso à base de dados, permitindo que os usuários acessem somente aquela que foi atribuída a seu login.

No cliente, foi iniciada a aplicação workbench inserindo as informações de usuários, senha e endereço do servidor. Após isso entrou-se na database “Usuários”, a qual foi adicionado uma base de informação com 6 colunas e 12.000 linhas na tabela SERVIDORES e outra tabela de referência chamada de DADOS_PESSOAIS, como é mostrado na figura 21.

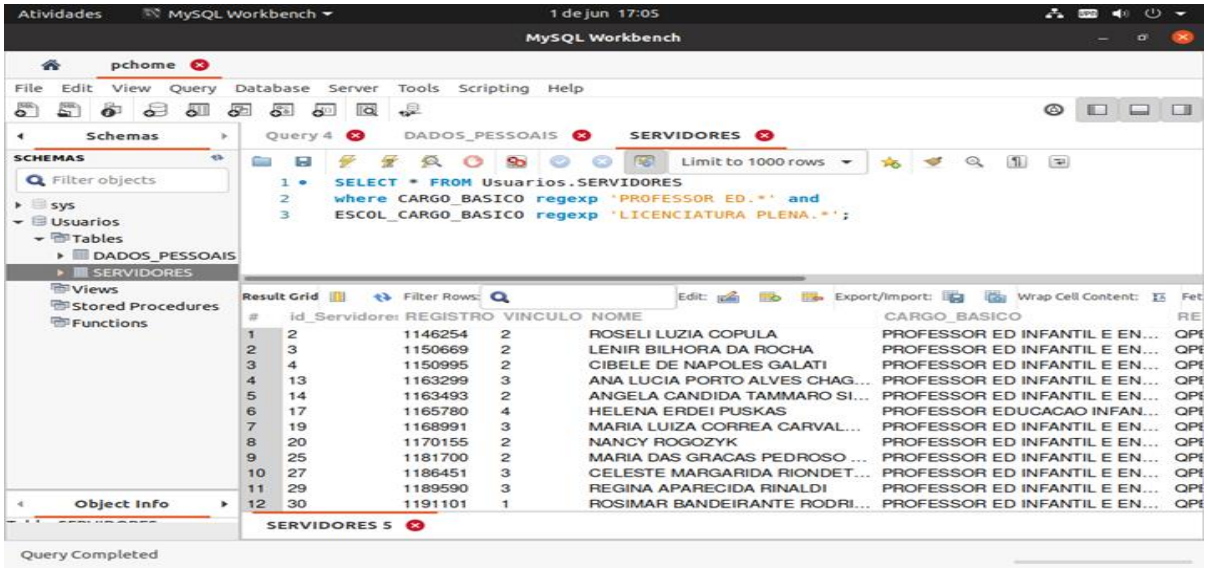
Figura 21 - Visão da base de dados no Windows



Fonte: Autoria Própria, 2021

Feito isso, foi criada uma consulta na linguagem SQL para geração de relatório em diversos formatos de arquivo como pdf e csv. Essa linguagem buscar determinados conjunto de dados conforme a necessidade dos usuários, enquanto os formatos gerados permitem usuários ter uma visão completa sobre os dados, manipulá-los em aplicativos da nuvem (Google Docs e Office 365), além disso, criar informações para auxiliar no processo decisório de determinado setor da empresa.

Figura 22 - Visão do banco de dados no sistema operacional Linux



Fonte: Autoria Própria, 2021

8 CONSIDERAÇÕES FINAIS

Segundo Delfino (2017), o PfSense tornou-se uma ferramenta muito utilizada, atingindo mais de 1 milhão de instalações no mundo inteiro desde seu início. Desse modo, no projeto elaborado, essa ferramenta mostrou-se muito eficiente e de fácil compreensão, com ferramentas manipuláveis para usuários que necessitam de aplicações para manipular dados hospedados na rede local da empresa, interface gráfica que facilita administração da rede remotamente e inúmeras aplicações complementares capazes melhorar e prover segurança no acesso aos dados de servidor por meio da internet durante a pandemia da covid-19.

Além disso, o software Pfsense mostrou-se eficiente no processo de acesso e tráfego da VPN, possibilitando usá-la em tarefas que exigem muito processamento de dados como no banco de dados, acesso a pasta compartilhadas em setores e áreas, e gerenciar uma rede de grande infraestrutura remotamente sem a necessidade de esta presencialmente com uso da VPN.

Foram encontradas algumas dificuldades na configuração de rede da provedora de acesso, pois essa limita o uso de endereços NAT para rede externa, e também com as configurações padrões do roteador da operadora que dificulta estabelecer um endereço estático para servidor, por exemplo. Quanto ao Pfsense, houve problema no tempo de expiração do certificado SSL – responsável por assegurar ao servidor que usuário está cadastrado e atualizado suas credenciais no serviço – que foi resolvido com aumento no tempo de validade deste mecanismo de segurança e alteração nos certificados dos clientes.

REFERÊNCIAS

BOZOVIC, N. **What is OpenVPN**? – A Beginners-Friendly Guide to OpenVPN, The Most Popular VPN Protocol!. 2019. Disponível em: <https://www.technadu.com/openvpn/8640/>. Acesso em: 06 Mar.2021.

CANALTECH. **O que é PPPoE**. 2017. Disponível em Canaltech: <https://canaltech.com.br/produtos/O-que-e-PPPoE/>. Acesso em: 29 Mar. 2021.

CETICBR. **Painel TIC Covid-19**. Nov. 2020. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20201104182616/painel_tic_covid19_3edicao_livro%20eletr%C3%B4nico.pdf/>. Acesso em: 18 Mar 2021.

DELFINO. Pedro. **PfSense** – Principais Vantagens e Recursos dessa poderosa ferramenta de Firewall. 2017. Disponível em: <https://e-tinet.com/linux/pfsense-vantagens/>. Acesso em: 11 Jun. 2021.

DGTI. IFCE. **Firewall**: Regras. 2021. Disponível em: http://docs.dgti.ifce.edu.br/lib/exe/fetch.php?cache=&media=pfsense:firewall-rules-lan.png. Acesso em: 3 Abr. 2021.

FERNANDES, Mirian. **Balanceamento de Links:** Tudo que você precisa saber!. 2019. Disponível em: <https://blog.starti.com.br/balanceamento-de-links/>. Acesso em: 27 Mar. 2021.

_____. **Firewall Appliance**: é viável para sua empresa?. Set. 2019. Disponível em: <https://blog.starti.com.br/firewall-appliance/>. Acesso em: 27 Nov. 2021.

_____. **Proxy**: Tudo o que você precisa saber!. Out. 2019. Disponível em: <https://blog.starti.com.br/proxy/>. Acesso em: 26 Mar. 2021.

FIREWALLS. **What is a UTM Firewall?.** Disponível em: <https://www.firewalls.com/what_is_utm_firewall>. Acesso em: 22 Mar. 2021.

FIREWALLS. 2021. Disponível em: https://www.firewalls.com/pub/media/wysiwyg/pages/what-is-utm.png. Acesso em: 20 Jun. 2021.

FOROUZAN, Behrouz. A. **Comunicação de Dados e Redes de Computadores** (4 ed.). AMGH Editora, 2008.

FREEBSD. **Software License Policy.** Disponível em: <https://www.freebsd.org/internal/software-license/>. Acesso em: 22 Mar. 2021.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa** (4.ed.). São Paulo: Altas S.A. 2008. Disponível em: <http://www.uece.br/nucleodelinguasitaperi/dmdocuments/gil_como_elaborar_projeto_de_pesquisa.pdf>. Acesso em: 05 Mai. 2021.

_____. **Métodos e Técnicas de Pesquisa Social** (6 ed.). São Paulo: Atlas S.A, 2008. 50 p.

HENRIQUES, Pedro. **Firewall pfSense**: entenda como funciona essa solução de segurança. 2020. Disponível em: <https://indicca.com.br/firewall-pfsense-2/>. Acesso em: 24 Mar. 2021.

IDTECNOLOGIA. **Firewall Appliance para empresas**. Ago. 2020. Disponível em: <https://blog.idtecnologia.com.br/firewall-appliance-para-empresas/>. Acesso em: 27 Mar. 2021.

KAGUTECH. **DNS Dinamico**: Configuração. Abr. 2021. Disponível em: <https://por.kagutech.com/4252775-dynamic-dns-setup>. Acesso em: 26 Mar. 2021.

MILIN-ASHMORE, J. **O WireGuard é o futuro dos protocolos de VPN**?. Fev. 2021. Disponível em: <https://pt.vpnmentor.com/blog/o-wireguard-e-o-futuro-dos-protocolos-de-vpn-atualizacao-de-seguranca/>. Acesso em: 25 Mar. 2021.

NETGATE. **Captive Portal**. Set. 2020. Disponível em: <https://docs.netgate.com/pfsense/en/latest/captiveportal/index.html/>. Acesso em: 5 Mar. 2021.

_____. **Choosing a VPN Solution**. Abr. 2021. Disponível em: <https://docs.netgate.com/pfsense/en/latest/vpn/selection.html>. Acesso em: 30 Abr. 2021.

_____. **Dynamic DNS**. Set. 2020. Disponível em: <https://docs.netgate.com/pfsense/en/latest/services/dyndns/index.html>. Acesso em: 26 Mar. 2021.

_____. **Network Address Translation**. Set. 2020. Disponível em: <https://docs.netgate.com/pfsense/en/latest/nat/index.html/>. Acesso em: 27 Mar. 2021.

_____. **PPPoE Server**. Set. 2020. Disponível em: <https://docs.netgate.com/pfsense/en/latest/services/pppoe-server.html>. Acesso em: 29 Mar. 2021.

NETO, Rodolfo Teixeira. **IPsec Vs. SSL VPN**: Comparando Velocidade, Segurança e Tecnologia. Jan. 2020. Disponível em: <https://dominandoredes.com.br/ipsec-vs-ssl-vpn/>. Acesso em: 26 Mar. 2021.

OPAS. Organização Pan-Americana. **Folha informativa sobre COVID-19**. Disponível em: <https://www.paho.org/pt/covid19/>. Acesso em: 11 Jun. 2021.

PFSENSE. **Take A Tour Pfsense**. Disponível em: <https://www.pfsense.org/about-pfsense/>. Acesso em: 5 Mar.2021.

RAIDBR. **Firewall UTM**: 5 benefícios para analistas e gestores de tecnologia. 2019. Disponível em: <https://raidbr.com.br/firewall-utm-5-beneficios-para-analistas-e-gestores-de-tecnologia/>. Acesso em: 24 Mar. 2021.

RFC 2131. **RFC 2131 - Dynamic Host Configuration Protocol**. Mar. 1997. Disponível em: https://tools.ietf.org/html/rfc2131>. Acesso em: 5 Mar. 2019.

STRN. **Balanceamento de Carga do Servidor.** 2020. Disponível em: <https://strn.com.br/pfsense/loadbalancing/>. Acesso em: 27 Mar. 2021.

TEAM, C. **Licença BSD**. 2012. Disponível em: <https://wiki.ncrcolibri.com.br/pages/viewpage.action?pageId=33587283>. Acesso em: 24 Mar. 2021.

WILLIAMSON, Matt. **Um guia prático com exemplos ilustrados de configurações, para usuários iniciantes e avançados sobre o PfSense 2.0**. 2012. (C. Persaud, Trad.).