PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA
GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO

UM ESTUDO DOS SOFTWARES ENDIAN FIREWALL E PFSENSE FIREWALL

RAFAEL DOS SANTOS DOURADO

GOIÂNIA
2022

RAFAEL DOS SANTOS DOURADO

UM ESTUDO DOS SOFTWARES ENDIAN FIREWALL E PFSENSE FIREWALL

Trabalho de Conclusão de Curso apresentado à Escola Politécnica, da Pontifícia Universidade Católica de Goiás, como parte de requisitos para obtenção do título de Bacharel em Ciências da Computação.

Orientadora: Profa. Dra. Solange da Silva.

GOIÂNIA
2022

UM ESTUDO DOS SOFTWARES ENDIAN FIREWALL E PFSENSE FIREWALL

Este Trabalho de Conclusão de Curso julgado adequado para obtenção o título de Bacharel em Ciências da Computação, e aprovado em sua forma final pela Escola Politécnica, da Pontifícia Universidade Católica de Goiás, em __/_____/_____.

_____

Profa. Ma. Ludmilla Reis Pinheiro dos Santos
Coordenadora de Trabalho de Conclusão de Curso

Banca Examinadora:

_____

Orientadora: Profa. Dra. Solange da Silva

_____

Prof. Me. Rafael Leal Martins

_____

Prof. Me. Wilmar Oliveira de Queiroz

GOIÂNIA
2022

AGRADECIMENTOS

Aos meus pais, Maura e Adair, que foram meus pilares, investiram e me motivaram nesta jornada.

Ao meu irmão, Gabriel, que me incentivou e me ajudou nas horas mais difíceis.

À minha esposa e companheira, Marta Larissa que esteve ao meu lado em toda a minha trajetoria.

À toda minha família e amigos que colaboraram de alguma forma para ser quem eu sou hoje.

À OVG, que me ajudou com a bolsa estudantil,permitindo a a minha graduação e formação profissional.

À minha prezada e querida orientadora Profa. Dra. Solange da Silva, pelos seus ensinamentos, conhecimentos, atenção e compreensão para realização deste trabalho.

Agradeço a todos que, de uma forma ou de outra, contribuiram para que este trabalho fosse realizado.

RESUMO

O objetivo deste trabalho foi o de **i**dentificar e descrever as funcionalidades dos *firewall Pfsense e Endian,* usados em redes de computadores. Entretanto, este estudo focou mais no *Endian Firewall*, por este ser menos explorado na literatura. As funcionalidades mais usadas no *Endian Firewall* são: Sistema de Prevensão de Intrusão, Servidor DCHP, Proxy Bloqueio de domínios e ignorar o proxy transparente. Foi descrito o seu funcionamento, além de testar sua eficácia em um ataque, usando a ferramenta Nmap. O estudo permitiu concluir que o *Endian Firewall* é eficaz e atende aos requisitos para que uma rede de computadores possa ser protegida e organizada. Usando o sistema operacional Kalli Linux e a ferramenta Nmap, foi possivel demonstrar que o *Endian Firewall* possui funcionalidades que realmente funcionam para bloquear os ataques ou acessos não permitidos.

Palavras Chaves: Redes de computadores. Segurança da Informação. *Firewall*. *Softwares* de Segurança.

ABSTRACT

The objective of this work was to identify and describe the functions of the Pfsense and Endian firewalls, used in computer networks. However, this study focused more on the Endian Firewall, as it is less explored in the literature. The most used functionalities in Endian Firewall are: Intrusion Prevention System, DCHP Server, Proxy Domain blocking and transparent proxy bypass. Its operation was described, in addition to testing its effectiveness in an attack, using the Nmap tool. The study concluded that the Endian Firewall is effective and meets the requirements for a computer network to be protected and organized. Using the Kalli Linux operating system and the Nmap tool, it was possible to demonstrate that Endian Firewall has features that really work to block attacks or unauthorized access.

Key words: Computer networks. Information Security. *Firewall*. Security *Software*.

LISTA DE FIGURAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil
CPU	*Central Processing Unit* ou Unidade de Central de Processamento
DNS	*Domain Name System* ou Sistema de Nomes de Domínio
DVD	*Digital Versatile Disc* ou Disco Digital Versátil
FTP	*File Transfer Protocol* ou Protocolo de Transferência de Arquivos
GB	Gigabyte
GHz	GigaHertz
GPL	*General Public License ou* Licença Pública Geral
HTTP	*Hypertext Transfer Protocol* ou Protocolo de Transferência de Hipertexto
HTTPS	*Hyper Text Transfer Protocol Secure* ou Protocolo de Transferência de Hipertexto Seguro
IEC	*International Electrotechnical Commissio*n ou Comissão Eletrotécnica Internacional
IP	*Internet Protocol* ou Protocolo da Internet
ISO	*International Organization for Standardization* ou Organização Internacional de Normalização
LAN	*Local Area Network* ou Rede Local
LGPL	*Lesser General Public License* ou Licença Pública Geral Menor
NMAP	Network Mapper ou Mapeador de rede
NAT	*Network Address Translation* ou Traduções de endereços de rede
OSS	*Software open source* ou *Software* de código aberto
POP3	*Post Office Protocol* ou Protocolo dos Correios
SGSI	Sistema de Gestão de Segurança da Informação
SMTP	*Simple Mail Transfer Protocol* ou Protocolo de Transferência de Correio Simples
SSH	*Secure Socket Shell* ou Shell de soquete seguro
SI	Segurança da Informação
TCP	*Transmission Control Protocol* ou Protocolo de Controle de Transmissão
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
URL	*Uniform Resource Locator* ou Localizador Uniforme de Recursos

USB	*Universal Serial Bus* ou Porta Serial Universal
UTM	*Unified Threat Management* ou Gerenciamento Unificado de Ameaças
VPN	*Virtual Private Network* ou Rede Virtual Privada
WAN	*Wide Area Network* ou Rede de longa distância
WEB	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

Com o surgimento das redes de computadores a organização dos sistemas computacionais foi completamente modificada. Inicialmente, os sistemas computacionais eram organizados tendo como base um único computador responsável por executar todo o processamento e armazenamento necessários (FRANCISCATTO, 2018).

Durante os últimos trinta anos, as tecnologias voltadas às redes de computadores têm evoluído com o objetivo de dar suporte a crescente dependência da humanidade pela computação (OROZCO, 2018).

Na Era da Informação há o grande desafio da Segurança da Informação (SI). Pessoas, empresas, governos, países e instituições estão sujeitas a sofrerem variados incidentes com uma grande amplitude de impactos. Isso torna mais complexa a tarefa de proteção da informação (NAKAMURA, 2016).

A especificação e a implementação do Sistema de Gestão de Segurança da Informação (SGSI) de uma empresa é influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos e o tamanho da estrutura da organização (ABNT, 2006).

“A SI é a proteção de um complexo de dados disponíveis no interior de uma organização” (RAMOS et al., 2018, pág 58). A SI faz com que pessoas não autorizadas não consigam as informações ou sistemas das instituições, impedindo que dados sejam roubados, danificados ou destruídos. Assim, podem garantir o desenvolvimento do negócio, aumentando sua credibilidade e segurança (PAZ, 2021).

Os dados são um conjunto de informação que permite chegar ao conhecimento de algo, podem ser considerados dados, por exemplo, documentos, filmes, livros, imagens e outros (MOREIRA et al.,2020).

O objetivo da segurança de dados é protegê-los contra ameaças, roubos, acidentes, destruição entre outros. Segurança de dados trata-se da preservação das informações de uma organização e precisa ser uma preocupação não só da equipe de Tecnologia da Informação (TI), mas de todos os funcionários da empresa (LUCENA, 2017).

O *Firewall* é uma combinação de *hardware* e *Software* que tem o objetivo de isolar a rede local de uma organização da Internet. Com ele é possível implementar

uma política de controle de acesso, bloqueando ou permitindo o trafego de dados, resultando em segurança (RAULINO, 2019).

O uso do *firewall* é importante para proteger redes de computadores, pois *firewalls* atuam como a primeira linha de defesa. Uma das funcionalidades dos *firewalls* é a filtragem de pacotes. De acordo com regras inseridas pelo administrador da rede, ele tem o total controle dos dados (GUERRA ,2019).

É relevante estudar esse tema por que a SI é muito importante para a sobrevivência de empresas no mercado, principalmente por causa do uso da Internet (RAMOS et al, 2018). Além disso, a SI é um ponto de grande importância e cuidado por parte das empresas que desejam proteger todos os dados de sua instituição, um fator indispensável para o exercício de qualquer atividade empresarial (ZEFERINO, 2020).

Diante deste contexto, esse projeto visa responder a seguinte questão de pesquisa: **- Quais as funcionalidades dos *firewall Pfsense e Endian* para segurança das redes de computadores?**

Este trabalho tem o objetivo geral de **i**dentificar e descrever a funcionalidade dos *firewall Pfsense e Endian* para redes de computadores.

Os objetivos específicos são:

- Descrever o funcionamento do *firewall firewall Pfsense e Endian;*
- Fazer um passo a passo para instalar dos softwares *Endian Firewall e do Kali Linux;*
- Realizar ataques para testar a eficacia do *Endian Firewall.*

Espera-se que os resultados deste trabalho possam contribuir:

- Informando aos administradores de redes ou usuários sobre alguns *firewall* que possam garantir a segurança da informação, tanto em redes corporativas quanto domesticas;
- Trazendo informações de segurança para os usuários de redes de computadores;
- Mostrando a importância de se ter Políticas de Segurança de dados em uma empresa;
- Apresentando as normas de segurança existentes.

Quantos aos aspectos metodológicos, a natureza desta pesquisa é um

resumo de assunto. Quanto aos seus objetivos é uma pesquisa exploratória e descritiva. Em relação aos procedimentos técnicos é uma pesquisa bibliográfica e experimental.

Esta monografia está organizada em 7 capítulos, sendo estruturada da seguinte forma: O Capítulo 1 apresenta a introdução com o contexto do trabalho, a questão depesquisa, objetivos e resultados esperados. O Capítulo 2 apresenta o referencial teórico com conceitos, definições e trabalhos relacionados com o tema. No Capítulo 3 estão descritos os procedimentos metodológicos, mostrando como e o que foi feito para atingir o objetivo geral. O Capítulo 4 descreve os *Softwares Pfsense* e *Endian Firewall*, mostrando suas funcionalidades. O capítulo 5 traz os experimenttos realizados, testando a eficácia do Endian. Finalmente. O capítulo 6 descreve as configurações das funcionalidades do Endian *firewall.* O Capítulo 7 traz as considerações finais e sugestões para continuidade desta pesquisa.

2 REFERENCIAL TEÓRICO

Este capítulo é composto por duas partes: a primeira apresenta os conceitos e definições da área e a segunda trazendo alguns trabalhos relacionados ao tema.

2.1 Segurança da Informação

Com a grande evolução das comunicações entre empresas, a transferência de informações se torna mais rápida a cada dia, e isso traz grandes lucros as empresas que fazem uso desses mecanismos, porém junto com essa evolução, tem pessoas que usam essa evolução para furtos de informações e até mesmo de serviços e produtos (MARCIANO, 2016).

A SI se refere à proteção existente sobre os dados de informações de uma determinada empresa ou pessoa, por tanto as informações podem ser corporativas quanto às pessoais, cada uma com seu determinado valor (SANTOS, 2016)

O objetivo da SI é buscar aplicar práticas e políticas de segurança que garantam a integridade das informações corporativas, evitando possíveis vazamentos de dados, ataques, dentre outras ameaças que podem prejudicar a empresa (IBMEC, 2021).

Segundo Silva, Carvalho e Torres (2003), a utilização da SI surgiu de técnicos de sistemas de informática, no início do desenvolvimento de sistemas, por conta do crescimento da utilização de computadores e pelo interesse das empresas em redes de computadores corporativas. Os princípios para a segurança na época foram o custo/benefício, a concentração a proteção em profundidade (BRANDÃO, 2021).

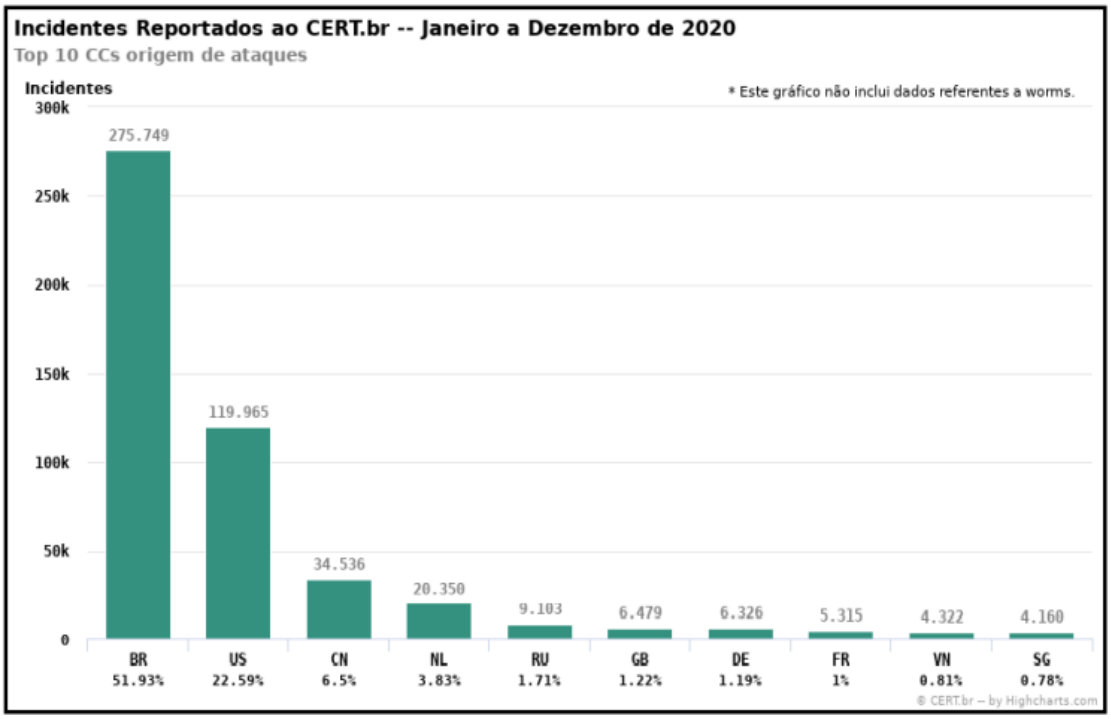
Em SI a palavra Ativo significa tudo que representa valor para a organização. Caso esse ativo seja violado, trará impactos negativos para o funcionamento das atividades da organização. Os ativos podem ser as pessoas, os programas, os equipamentos, “enfim, tudo que na sua ausência gera transtornos, implicando no bom funcionamento dos negócios” (FERNANDES, 2013, p 23).

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR, 2020), entre os meses de janeiro e dezembro de 2020, 531.039 incidentes relacionados SI foram reportados, dos quais 275.749 (51,93% dos incidentes) tiveram origem no Brasil, conforme exibido na Figura 1 (BRANDÃO, 2021)

Pode se observar na Figura 1 que o Brasil e os Estados Unidos lideram o

ranking de incidentes reportado, de janeiro a dezembro de 2020.

Figura 1 - Incidentes Reportados ao CERT.BR 2020



Fonte: CERT.BR, 2020.

2.2 Redes de Computadores

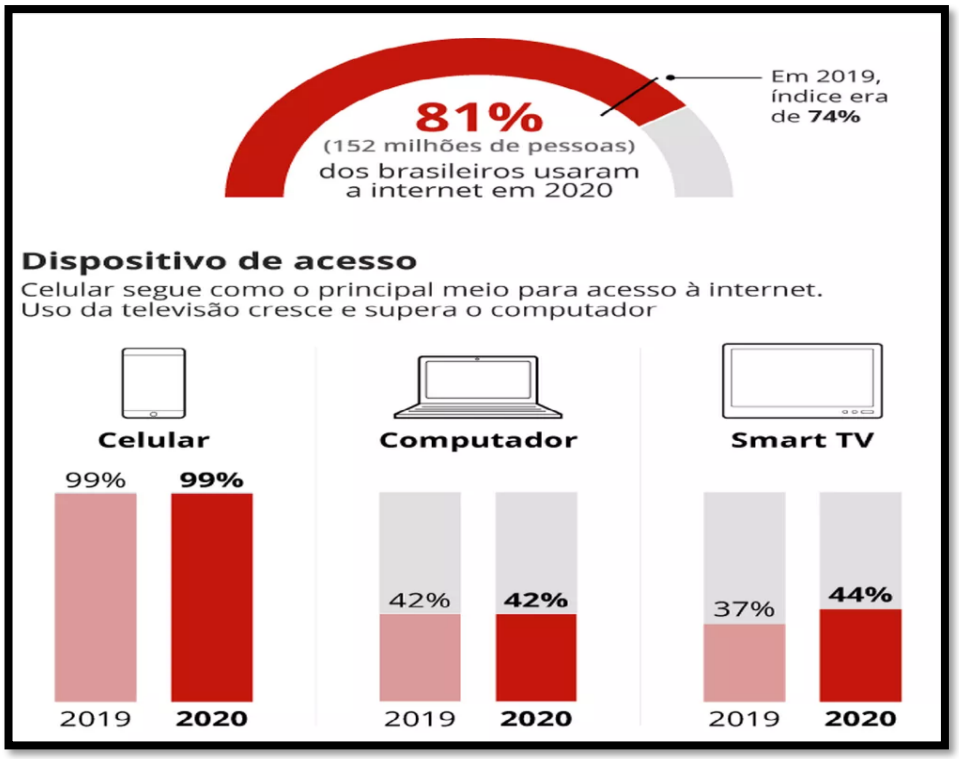
Redes de computadores são estruturas físicas (equipamentos) e lógicas (programas, protocolos) que permitem que dois ou mais computadores possam compartilhar suas informações entre si. Quando um computador está conectado a uma rede de computadores, ele pode ter acesso às informações que chegam nele e às informações presentes nos outros computadores ligados a ele na mesma rede. Isso permite um número muito maior de informações possíveis para acesso através daquele computador. As redes de computadores também potencializaram a forma de comunicação entre funcionários. Algumas empresas desempenham partes de suas atividades ou até mesmo serviços com base na dependência dessa comunicação (BOFF, 2015).

As redes de computadores domésticas se caracterizam principalmente por fazer parte de um grupo de dispositivos em uma pequena área. O uso doméstico de dispositivos para acesso à Internet para diversas atividades como uso pessoal, acesso a banco, redes social está crescendo a cada dia, a segurança desses dados

e conteúdo é fundamental (MACEDO et al., 2018).

Segundo a pesquisa da TIC Domicílios (2020) indica que 81% da população brasileira tem acesso a Internet em seus domicílios, como pode ser visto na Figura 2 (G1, 2022).

Figura 2 - Domicílios com acesso a Internet no Brasil



Fonte: Cetic.br, 2020.

Como pode ser vista na Figura 2 os celulares segue como os principais dispositivos usados para se conectar a internet.

2.3 Norma ISO/IEC 27000

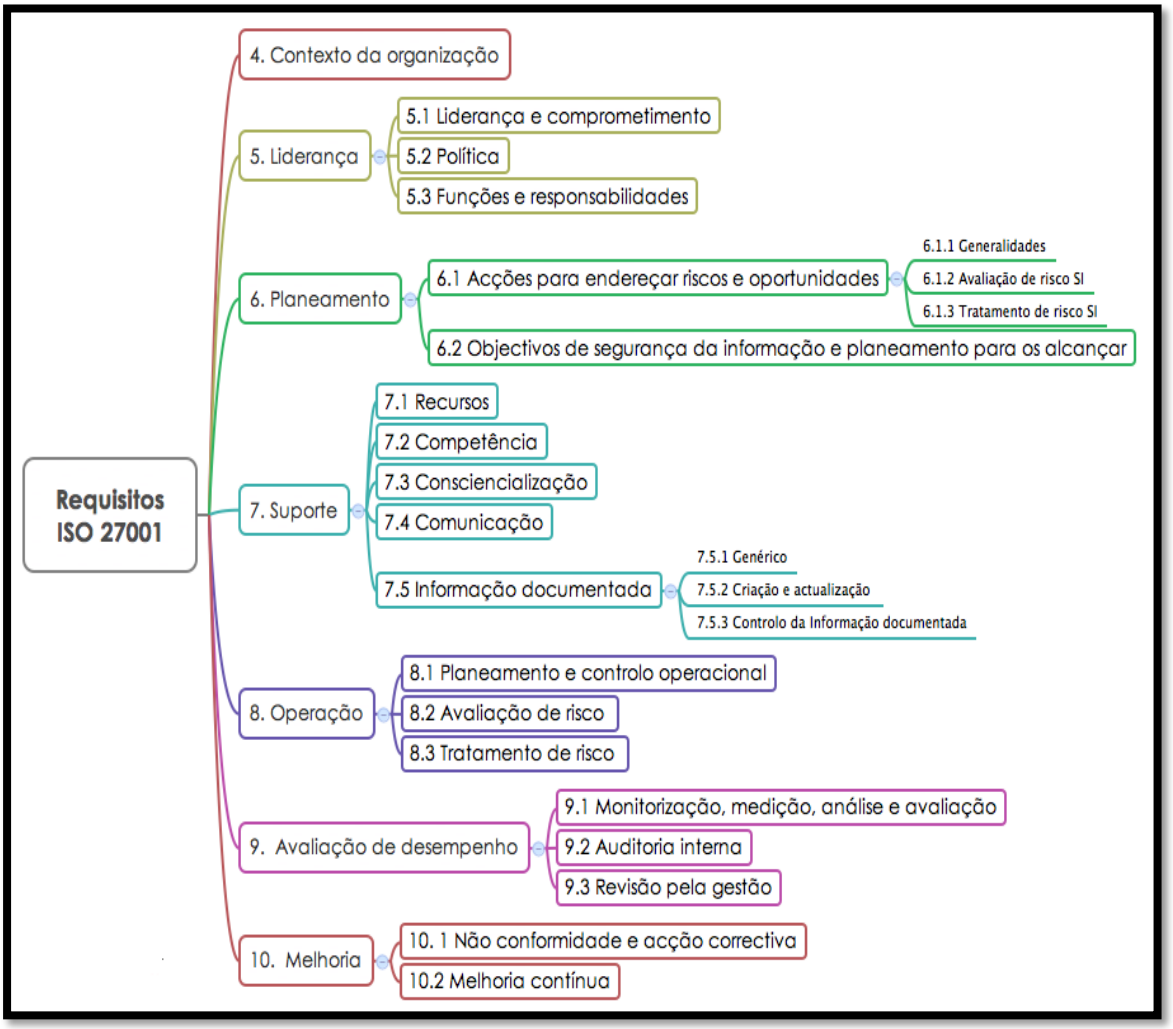
A segurança da informação é regulamentada pelas normas ISO/IEC 27000 e ISO/IEC 27001 que consistem em definir um propósito para o desenvolvimento de um Sistema de Gestão e Segurança da Informação (SGSI) nas organizações. Isso é imprescindível, tendo em conta a quantidade de informação produzida nas grandes corporações (ISO/IEC 27000, 2013).

A *International Organization for Standardization (ISO)*, ou seja, a Organização Internacional de Padronização, por meio da família da (ISO) 27000 aborda as normas para segurança da informação. Estas são convertidas para o SGSI, que criam

parâmetros para segurança dos armazenamentos eletrônicos e dados digitais (DEB SOLUTIONS TI, 2017).

A norma ISSO/IEC 27001:2013 especifica os requisitos, apresentada na Figura 3, para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação. Esta norma também inclui os requisitos para avaliação e tratamento dos riscos de SI voltados paras as necessidades da organização (TEIXEIRA, 2020).

Figura 3 - Requisitos da ISO 27001



Fonte: ABNT ISO 27001, 2013.

Observando a Figura 3 nota-se que os requisitos englobados são: o contexto da organização, liderança, planejamento, suporte, operação, avaliação de desempenho e melhoria.

2.3.1 Norma ISO/IEC 27002

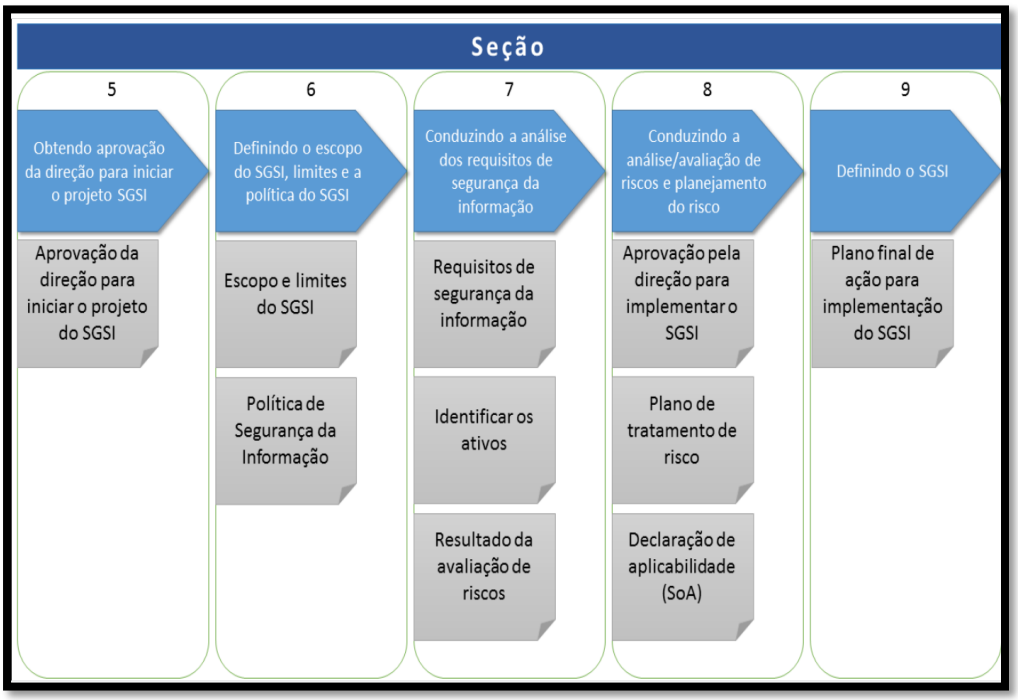
A ISSO/IEC 27002 é a norma que estabelece códigos de melhores práticas para apoiar a implantação de um SGSI nas organizações. Com o guia completos de implantações, ela descreve como os controles podem ser estabelecidos. Estes controles devem ser escolhidos com base em uma avalição de risco dos ativos mais importantes da empresa (OSTEC, 2020).

O principal objetivo da ISO 27002 é de estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Isso também inclui a seleção, a implementação e o gerenciamento de controles, levando em conta os ambientes de risco encontrados na empresa (OSTEC, 2020).

2.3.2 Norma ISO/IEC 27003

A ABNT ISO/IEC 27003:2011 possui as diretrizes para a implantação de um SGSI. Essa norma tem como objetivo mostrar como se faz a implantação de um SGSI, com foco na elaboração, planejamento e definição do projeto. Possui 5 fases, sendo cada fase separada por uma seção da norma, ilustrada na Figura 4 (LINO, 2016).

Figura 4 - Seções da ISO 27003

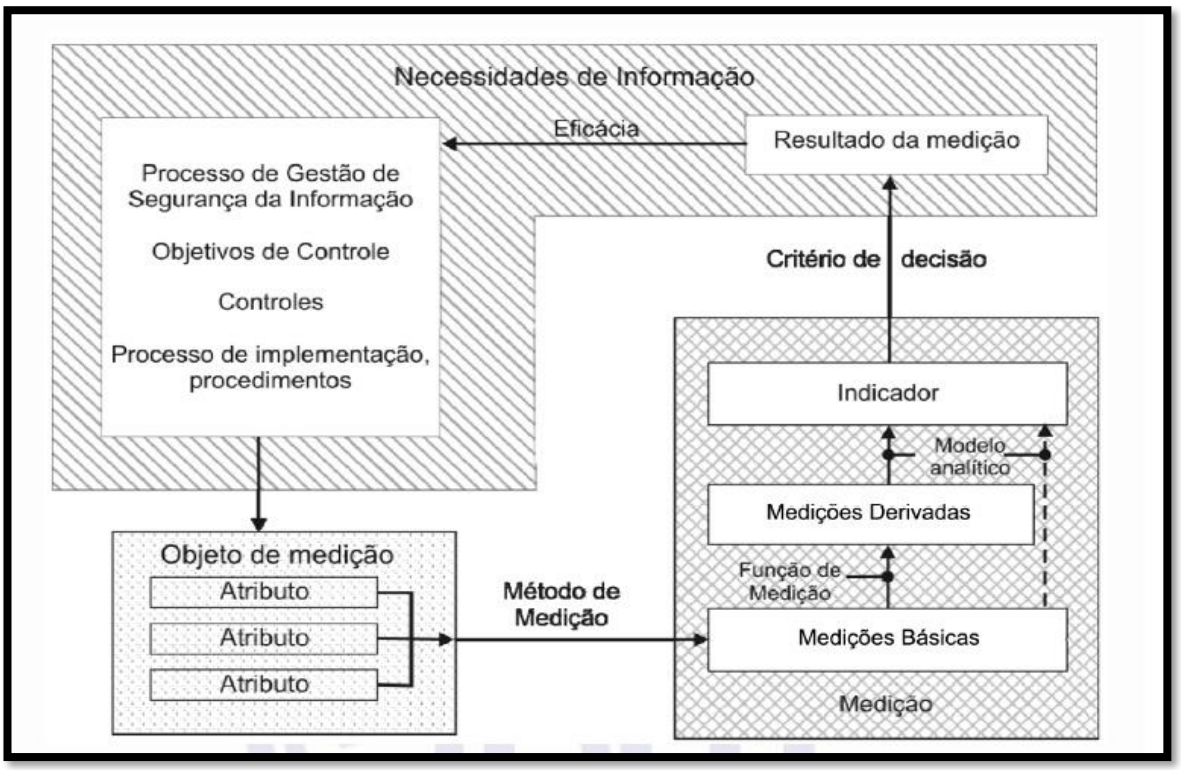


Fonte: ABNT ISO 27003, 2011.

2.3.3 Norma ISO/IEC 27004

A norma ABNT NBR ISO 27004:2010 foi publicada em 2010 e sugere padrões para desenvolvimento de métricas e medidas de desempenho para avaliar os SGSI. A norma fornece orientação e ajuda para as organizações, para que elas melhorem a eficácia e a eficiência dos seus SGSI, gerando dessa forma indicadores para medir o desempenho do SGSI. A norma cita todos os requisitos mínimos para um modelo de medição como definir o propósito da medição, os objetivos de controles, o objeto de medição e o processo para coleta e análise dos dados, mostrados na Figura 5 (LIMA, 2017).

Figura 5 : Modelo de medição da ISO 27004



Fonte: ABNT ISO 27004, 2010.

2.4 Blue Team e Red Team

O crescimento pela eficiência na segurança da informação fez com que as organizações passassem a lidar com o assunto de forma mais seria e estratégica. Tendo assim a formação de um *Blue Team* e um *Red Team*. as duas equipes proporcionam um trabalho de cibersegurança em nível mais elevado nas empresas. Cada uma delas tem sua importância e o alinhamento entre as duas traz muitos benefícios para empresa (COPYRIGHT, 2019).

Red team são profissionais de segurança ofensivos, especialistas em atacar sistemas e invadir as defesas. Red Teams são gupos internos ou externos dedicadas a testar a eficácia de um programa de segurança, emulando as ferramentas e técnicas de prováveis invasores da maneira mais realista possível (ACADITI, 2022).

As informações coletadas durante a fase de ateques são: Descobrir os sistemas operacionais em uso (Windows, macOS ou Linux). Identificar a marca e o modelo dos equipamentos de rede (servidores, *firewall*s, switches, roteadores, pontos de acesso, computadores, etc.), descobrir quais portas estão abertas ou fechadas em um *Firewall* para permitir ou bloquear tráfego específico (OSTEC, 2021).

Um Blue team, ou time azul, é uma equipe de especialistas em defesa cibernética. Sua atuação é focada em descobrir as melhores soluções para não ocorrer erros e falhas nos sistemas e redes corporativos e mitigar os riscos de ataques de cibercriminosos serem bem sucedidos e problemas como vazamento de dados e indisponibilidade de sistema acontecerem (ASER, 2022).

Enquanto um Red Team é formado com o objetivo de realizar testes de ciberataque que imitam tentativas de penetrar na rede e no sistema da empresa, o Blue Team é montado para se opor aos ataques simulados A responssabilidade do time azul é desenvolve estratégias para aumentar as defesas cibernéticas da organização, criando mecanismos de proteção da rede que tornam todo o ambiente virtual do negócio mais seguro (PAZ, 2019).

A equipe Blue Team primeiro coleta dados, documenta o que precisa ser protegido e realiza uma avaliação de risco. Eles então restringem o acesso ao sistema de várias maneiras, incluindo uma introdução de políticas de senha mais rígidas. Assim, a equipe pode garantir que estejam de acordo com os procedimentos de segurança. As ferramentas de monitoramento são frequentemente colocadas em prática, permitindo que as informações relacionadas ao acesso aos sistemas sejam registradas e verificadas (ACADITI, 2022).

2.5 Trabalhos Relacionados

O estudo de Brandão (2021) teve o objetivo de identificar problemas e riscos existentes nas redes sociais, simulando ataques com a tecnica de envios de email, para roubar dados pessoais. Identificou os problemas e os riscos associados às

redes sociais. Problemas de ataques relacionados a Engenharia Social, que utilizam métodos de *phishing, spyware*, cavalo de troia, *baiting* e dentre outras. Com os resultados da implementação realizada concluiu que os usuários são a porta de entrada para acontecer os cibercrimes. Portanto, precisam os usários ser conscientizados e capacitados, visando ficarem mais observadores e saberem como agir ao receber os cenários dos atacantes nas redes sociais.

Neves et al. (2014) mostraram que pesquisas e aplicações nescessárias para instalação e configuração de um *firewall* em *Software* livre chamado pfSense em empresas que possuam menos receita para gastos na área de segurança, mas que precisam de uma boa ferramenta de segurança. Com isso, eles concluiram que o projeto do *firewall* pfSense é viável, sendo a melhor solução *Open Source* pesquisada pela equipe, atendendo a demanda por segurança

O trabalho de Machado *(2021*) indentificou e descreveu algumas formas de ataques aos dados mais conhecidas, apresentando os pontos de vulnerabilidade do acesso. Quantos aos experimentos foram indentificados ataques do tipo: *Port Scanning Attack, Phishing, Spoofing, Sniffing* e SQL *Injection*. Seus resultados permitiram concluir que não existe uma única solução para evitar os ataques e resolver todos os problemas de vulnerabilidades da empresa, mas existem diversas formas e ferramentas eficientes que ajudam na proteção.

Em Gabriel (2021) foram apresentados estudos de caso de empresas que aplicaram a norma ISO 27005 em um sistema SGSI e realiza uma analise de vulnerabilidade. Com a combinação da ISO 27005 e NIST SP 800-30 geram probabilidade geral e avaliação dos riscos que, por fim, com auxílio de uma ferramenta de identificação de riscos, cria, a partir daquela combinação, uma tabela de avaliação e os métodos de resolução dos riscos encontrados. Seus resultados mostraram que a ISO 27005 não é um padrão imposto, mas sim uma recomendação de boas práticas que ajudam as empresas e organizações a proteger suas informações.

Azevedo (2019) apresentou um estudo de caso relatando a implantação do UTM *Endian Firewall Community* em uma rede empresarial. Isso resultou no aumento da segurança, maior controle sobre o tráfego da rede, aliado com baixo custo de implantação. Os módulos de *firewall* e *proxy* presentes no UTM elevaram a segurança por meio do controle de portas, de forma que somente aquelas que realmente eram utilizadas pela empresa ficassem abertas, evitando entradas

indesejadas na rede. Além disso, bloquearam o uso de redes sociais (facebook, youtube, etc), como uma regra de segurança na empresa.

3 MÉTODO

Esta pesquisa é um resumo de assunto, buscando explicar a área do conhecimento do projeto, mostrando sua evolução histórica, como resultado da investigação das informações obtidas, levando ao entendimento de suas causas e explicações (WAZLAWICK, 2014).

Segundo os objetivos é uma pesquisa exploratória e descritiva. As pesquisas descritivas descrevem as características de certo fenômeno ou população. Também pode ser elaborada com o intuito de identificar as relações entre as variáveis (GIL, 2017). A pesquisa exploratória é considerada como a primeira parte do processo de pesquisa, porque namairoia das vezes o autor não tem um objetivo ou hipótese definida (WAZLAWICK, 2014).

Segundo os procedimentos técnicos é uma pesquisa bibliográfica e experimental.

A pesquisa bilbiográfica foi realizada a partir de materiais já publicados, sendo eles livros, teses, materiais disponibilizados na Internet, revistas, entre outros. A pesquisa foi realizada em artigos, TCCs, sites, blogs,nas bases dos periódicos da CAPES e livros.

A pesquisa experimental consiste em estabelecer um objeto de estudo, escolher as variáveis que a influenciam e determinar as formas de controle e observar os efeitos que a variável gera no objeto. Realiza pelo menos um dos elementos que julga ser responsável pela circunstância que está sendo pesquisado (GIL, 2017).

Segundo Gil (2017) o passo a passo a ser seguido nesta pesquisa experimental foi o seguinte:

a) Formulação do problema: **- Quais as funcionalidades dos *firewall Pfsense e Endian* para segurança das redes de computadores?**

b) **Definição do plano experimental**: foi descrito alguns ataques usando o software Kali Linux em específico o (NMAP) *Network Mapper* ou Mapeador de rede, assim mostrando a vulnerabilidade do servidor sem o controle do firewall. Foram descritas as funcionalidades mais usadas, para deixar a rede de computadores organizada e protegida.

c) **Determinação do ambiente**: foi realizado um experimento atacando dois servidores Windows, que foram instalados em duas maquinas virtuais

(VM) diferentes. Os servidores foram configurados em rede interna, na qual o Endian *Firewall* fez o controle e gestão. Cada maquina estava configurada da seguinte forma: 3 GigaBytes (GB) de memória *Randon Access Memory* (RAM) , 3 processadores e 20 GB de armazenamento. A maquina na qual foi instalado o *Firewall* tinha as seguintes configurações: 4 GB de memória RAM, 2 processadores e 50GB de armazenamento .

d) **Coleta de dados**: Ao realizar o ataque, o *Kally linux* trouxe todas as portas abertas naquele host atacado. Assim, foi possivel capturar as vulnerabilidade do servidor.
e) **Análise e interpretação dos dados**: foi testado se o *Firewall* conseguiria realmente proteger o servidor.
f) **Redação do relatório**: registro da pesquisa no TCC.

4 *SOFTWARES PFSENSE E ENDIAN FIREWALL*

Este capítulo traz a descrição e o funcionamento do *firewall* nos *Softwares* PfSense e do *Endian*, porém o foco maior será no *Firewall Endian.*

4.1 Visão Geral do *Software* PfSense

Segundo os próprios criadores, o PfSense é um *Software open soucer* (OSS), ou seja, de código aberto. Ele foi baseado no projeto FreeBSD criado com intuito para ser utilizado como um *Firewall* e roteador (TECHLISE, 2020).

O FreeBSD é um sistema operacional compatível com diversas plataformas. Seu sistema oferece rede avançada, segurança, performance e recursos de compatibilidade, além de ser um *Software* livre (MONQUEIRO, 2018).

O freeBSD é muito parecido com Linux, com duas diferenças principais em escopo e licenciamento, o projeto fornecer um sistema completo, um kernel, drives de dispositivos utilidades de usuário e documentação (ATANAZIO, 2016).

O pfSense é um *firewall* com todas as funcionalidades dos principais *Softwares* pagos. Entretando com uma diferença importante: é um *firewall* gratuito. Dessa forma, tanto computadores pessoais quanto dispositivos de uma rede corporativa podem ser protegidos. Assim o sistema de monitoramento e segurança completo, sem pagar caro por isso (INDICCA.COM, 2022).

A sua interface de gerenciamento WEB proporciona muitas facilidades na configuração e no gerenciamento de nosso *firewall* permitindo ao administrador da rede a configuração de interfaces de forma simples, até o estudo e verificação de falhas através de leitura de logs. O gerenciamento inicial mostra uma série de informações sobre o *firewall*, como por exemplo, os estados das interfaces conectadas, os servidores de Sistema de nome de domínio ou *Domain Name System* (DNS), tabela de estados, uso da Unidade de Central de Processamento ou *Central Processing Unit* (CPU) e memória entre outras informações muito úteis para o administrador de redes encarregado pelo gerenciamento do *firewall* (NEVES et al., 2014).

Programas de *Software* livre, em geral, são de fácil acesso e tem suas licenças livres. São permitidas modificações em sua distribuição. As principais licenças de *Software* livre são Licença Pública Geral ou G*eneral Public License* (GPL) e Licença Pública Geral Menor ou *Lesser General Public License* (LGPL) (SABINO, 2011).

O *Software* pfSense, com a ajuda de um sistema de pacote, fornece a mesma funcionalidade ou até mais de um *firewall* comercial comum. Sem nem uma limitação, ele tem a total capacidade de substituir com sucesso todos os *firewalls* comerciais de grandes nomes, tais como a SonicWall e a Cisco Pix (ELECTRIC SHEEP FENCING, 2022).

De acordo com a configuração e/ou as necessidades, a ferramenta pode assumir o papel de:

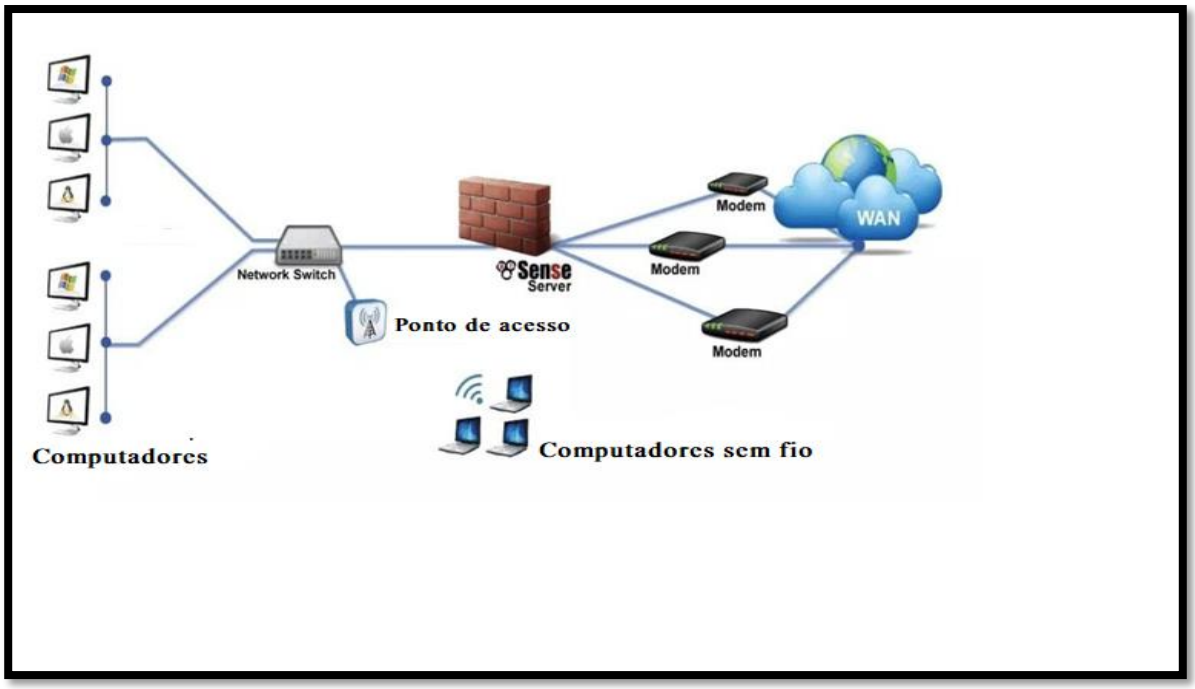
- *Firewall*;
- NAT;
- Ponto de Acesso *Wireless*;
- *Load Balancing* (Balanceamento de carga);
- VPN;
- *Reporting e Monitoring* (Relatório e Monitoramento);
- *Dynamic DNS* (DNS Dinâmico);
- *DHCP Server and Relay*;

4.2 Descrição do funcionamento do *Firewall* no *Software* pfSense

O pfSense é um *Software* livre customizado da distribuição do FreeBSD, sendo adaptado para uso como *firewall* e roteador, que é inteiramente gerenciado via interface WEB. Além de ser um poderoso *firewall*, e uma plataforma de roteamento. Ele possui uma variada lista de recursos que podem ser adicionadas através de *downloads* de pacotes permitindo assim a adição de funcionalidades de acordo com a necessidade do usuário (PFSENSE, 2022).

O *firewall* pfSense tem como objetivo monitorar o tráfego de uma rede, barrrando conteúdos potencialmente perigosos e proteger o dispositivo. Entretanto, esse monitoramento deve ser feito de forma cuidadosa, visando conteúdos maliciosos que devem ser contidos, como mostrado na Figura 6 (INDICCA.COM, 2022).

Figura 6 – Monitoramento Pfsense

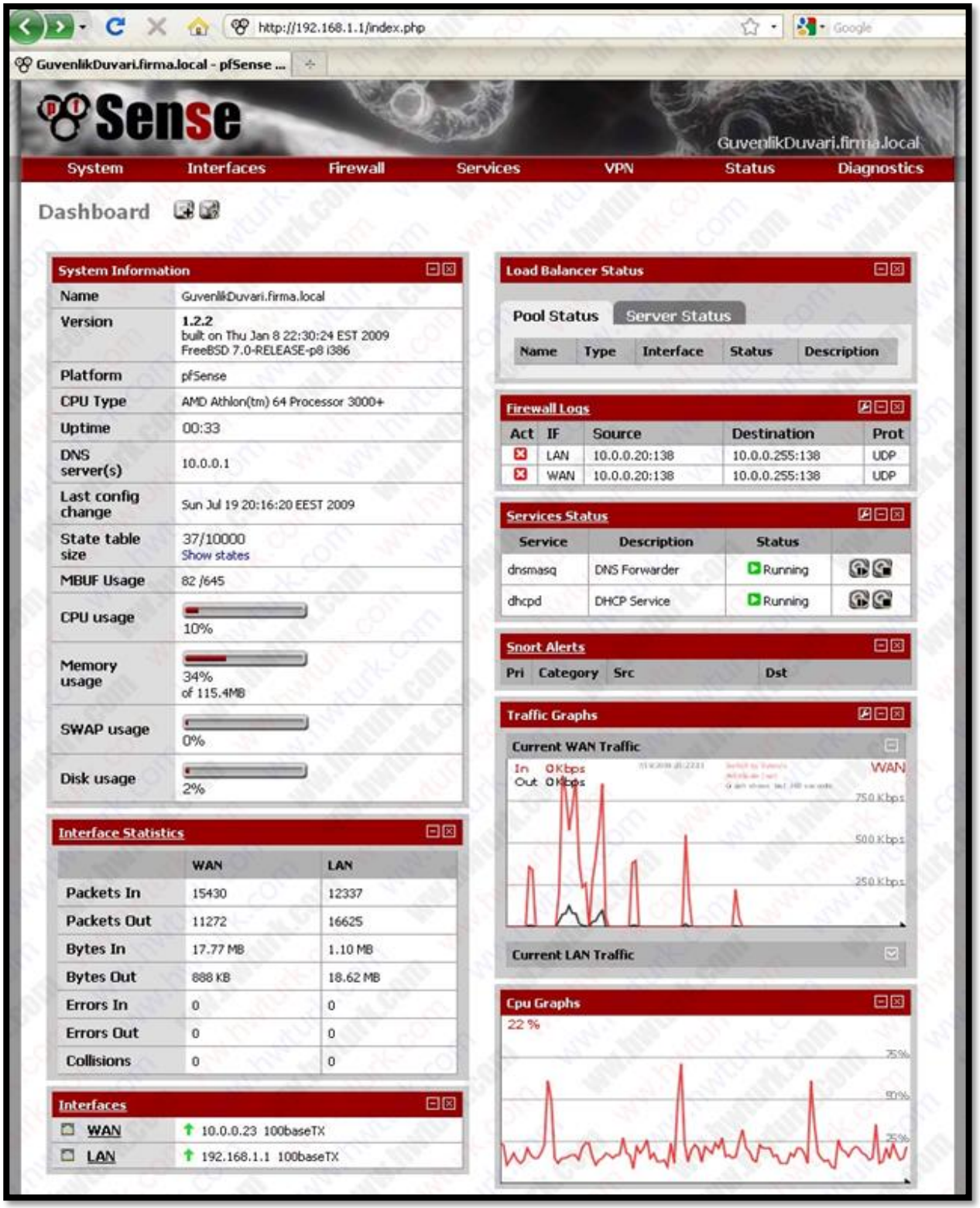


Fonte: MODIFICADO DE INDICCA.COM, 2022.

Na Figura 6 pode-se observar onde entra o pfsense na estrutura de rede. Ele atua como isolante da rede local com rede vermelhar ou rede WAN, trasendo maior segurança para os usuarios e para o administradaor da rede

A interface WEB do *Software* pfSense é dividida em abas de configuração com diferentes tipos de serviço, mostrada na Figura 7.

Figura 7 – *Dashboard Pfsense*



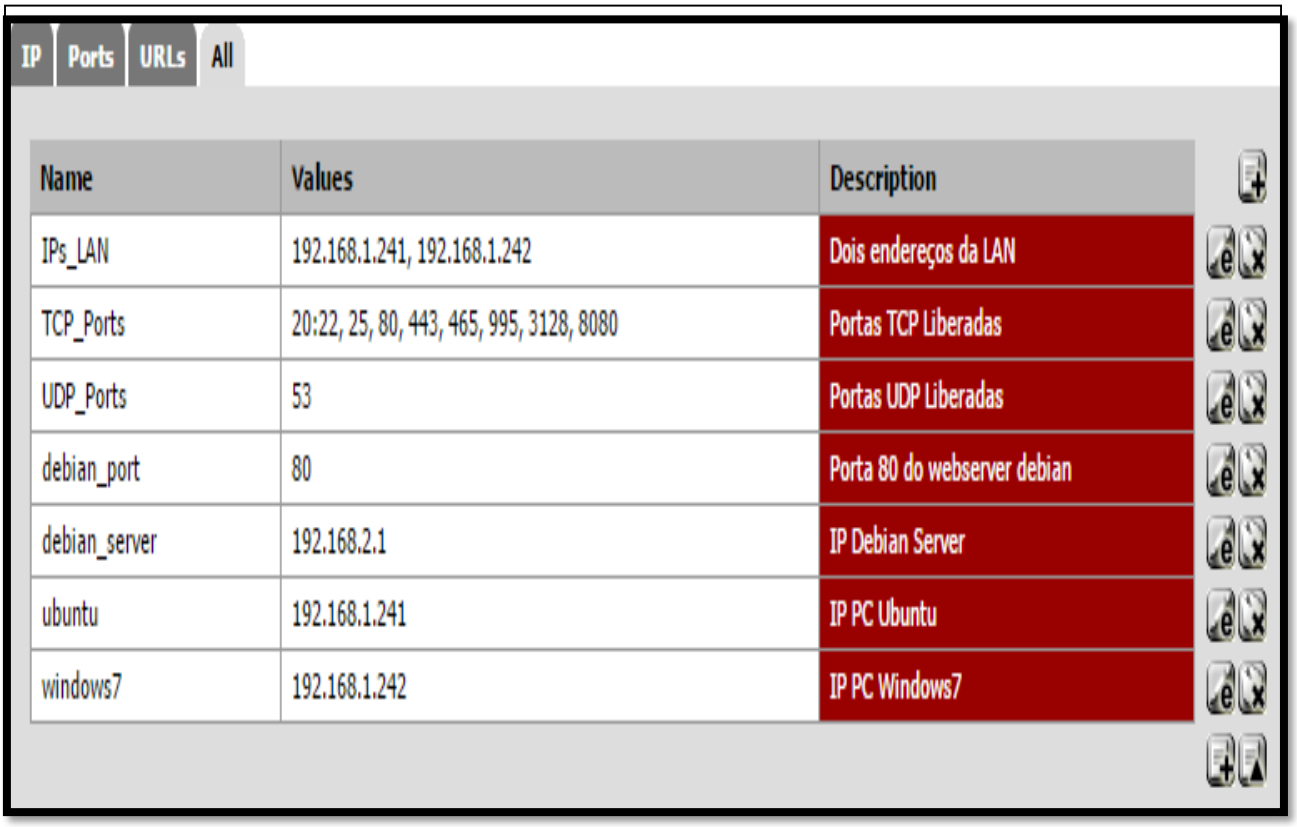
Fonte: PROFISSIONAIS TI, 2022.

Focando na aba do *firewall* tem as configurações que são consideradas mais importantes para o desenvolvimento de um *firewall* para empresas de pequeno e até mesmo médio porte.

Na aba *firewall* podem ser configuradas as regras de acesso à rede interna e quais requisições são possíveis de serem efetuadas para a rede externa. Nesta aba também são realizadas as configuração de *aliases*, que são grupos de hosts, redes ou portas que facilitam a administração de regras de acesso e Traduções de endereços de rede (NAT), tema que também é tratado nesta aba de configuração, através de *port forwarding* (NEVES et al., 2014)

Primeiramente aborda-se o *aliases. D*entro dessa opção há 3 tipos de agrupamento que demonstram grupos de endereços IP, portas de rede e URLs, como apresentado na Figura 8, existe a quarta aba mostrando todo os agrupamentos juntos.

Figura 8 – Agrupamento *Aliases*



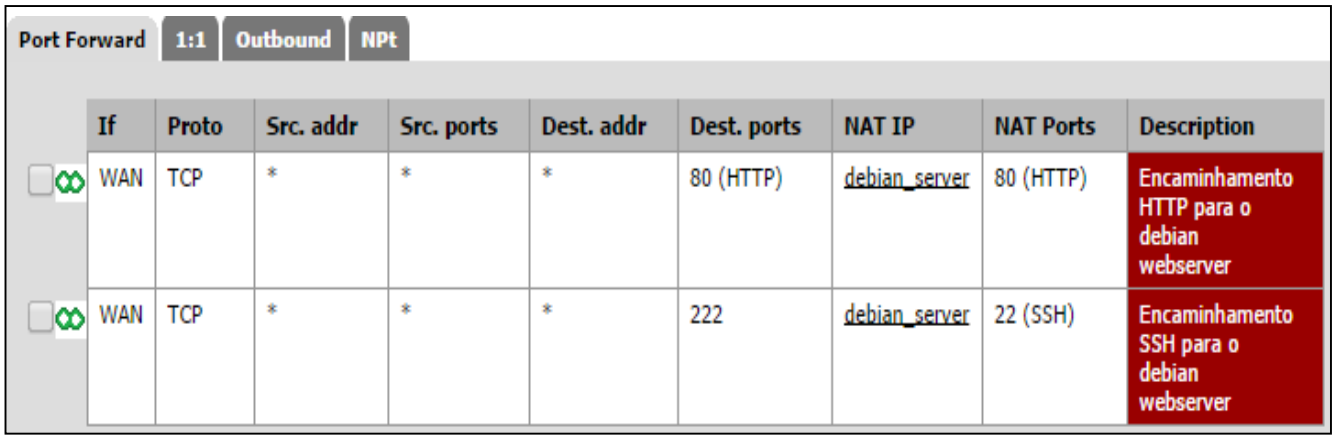
Fonte: SABOYA, 2021.

Na Figura 8 pode-se observar que ele faz as liberações de algumas portas padrões com 80, 53 e 443.

A segunda parte desta aba de configuração, as Regras de NAT e *port forwarding,* trata-se de um redirecionamento de portas de conexões vindo de uma rede externa para uma rede interna.

Na Figura 9, o exemplo consiste em redirecionar requisição partindo para o endereço IP externo, o endereço da interface Rede de longa distância (WAN), através da porta 80, para um servidor da pagina WEB dentro da rede, assim conseguindo acessar o servidor na rede interna (NEVES et al., 2014).

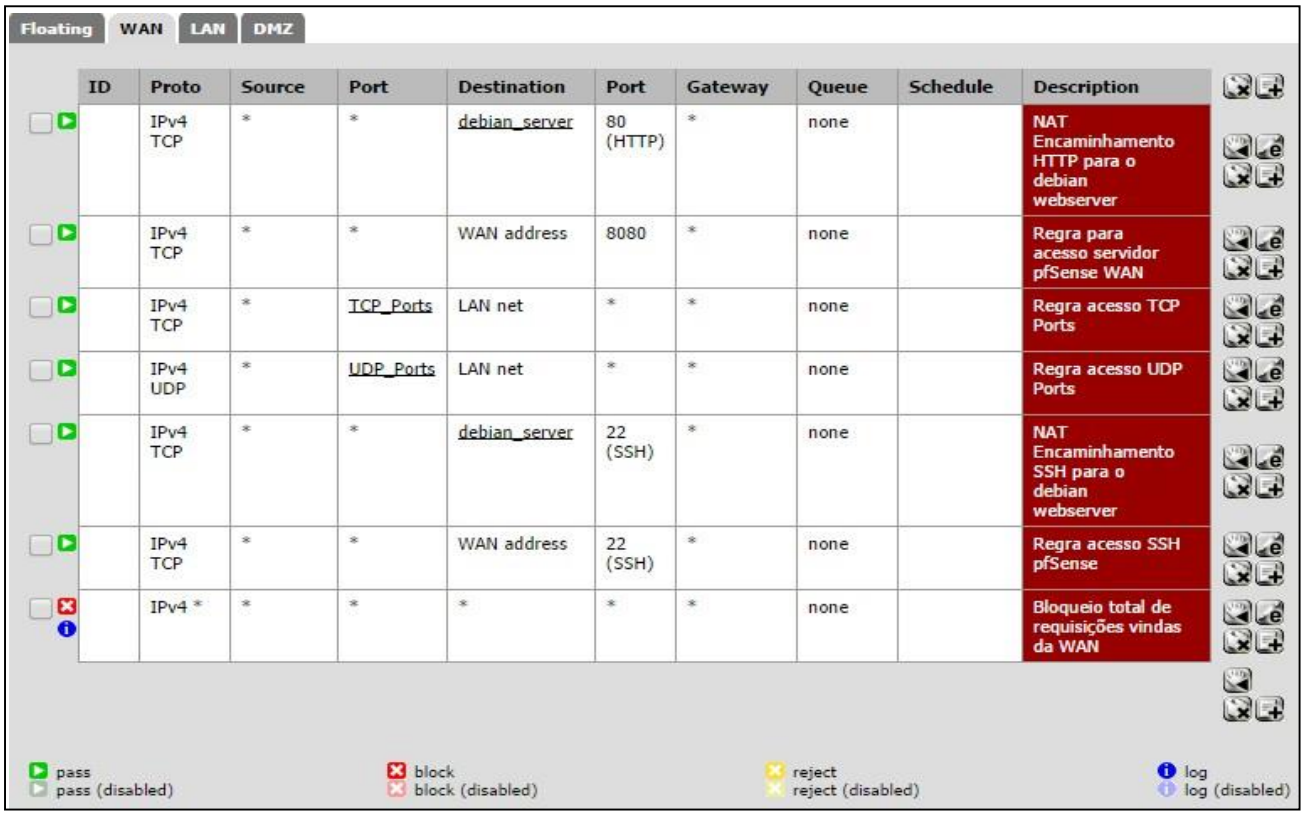
Figura 9 – Redirecionamento de porta



Fonte: NEVES et al, 2014.

Na opção regra de *Firewall,* ela é dividida por interfaces mostradas na Figura 10.

Figura 10 – Regras de *Firewall*



Fonte: NEVES et al,. 2014.

Podem ser criadas as regras específicas para cada interface. Um exemplo é que o endereço de uma rede local acesse somente determinadas portas para filtrar, somente páginas WEB, bloqueando tráfego para outros serviços. Podem ser também definidas regras que liberem o acesso somente a endereços IP conhecidos da empresa (NEVES et al., 2014).

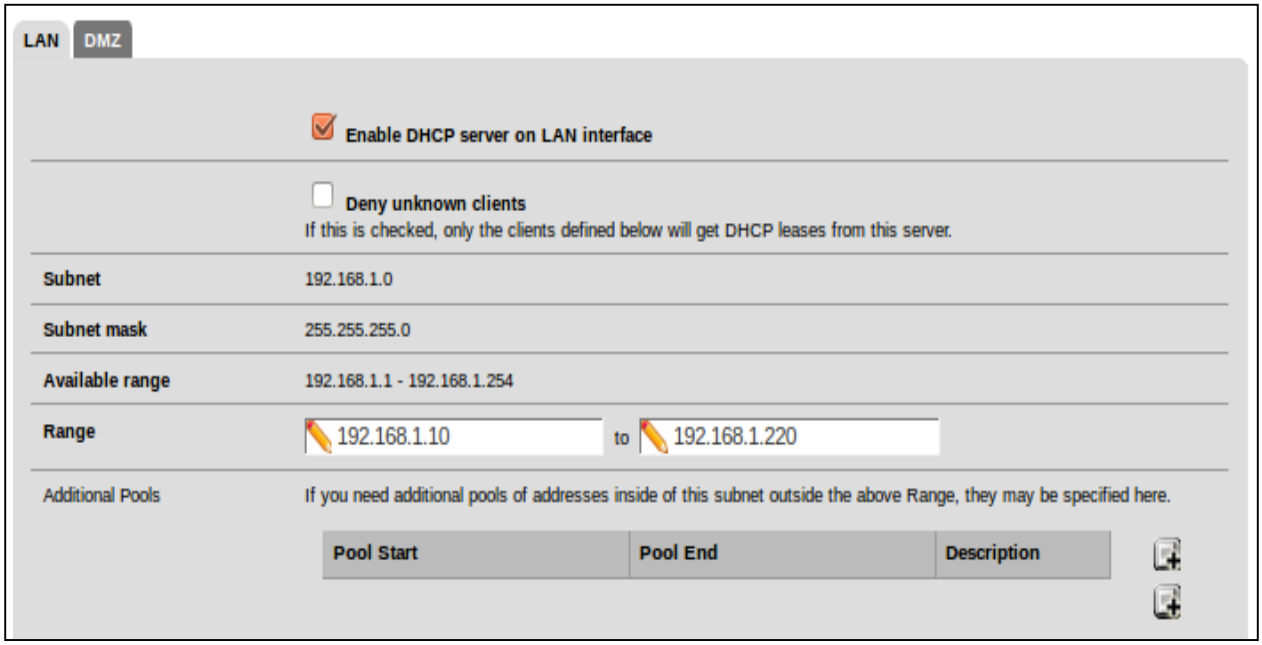
Com o servidor Protocolo de Configuração Dinâmica de Endereços de Rede (DHCP) Cada dispositivo conectado em uma rede baseada em TCP/IP deve ter um endereço IP unicast exclusivo para acessar a rede e seus recursos.

Sem o DHCP, os endereços IP teriam que ser configurados manualmente, mesmo sendo uma empresa de pequeno porte seria um trabalho grande para configurar um por um;

O servidor DHCP do pfSense auxilia na configuração da rede interna provendo endereços para os hosts da rede. No exemplo foi habilitado apenas servidor na interface de rede local ou Lan Area Netware (LAN).

Este servidor possibilita definir o range de endereços dinâmicos que será distribuído pelo nosso *firewall*, nesse caso serão os endereços compreendidos no intervalo de 192.168.1.10 até 192.168.1.220, ilustrada na Figura 11 (NEVES et al., 2014)

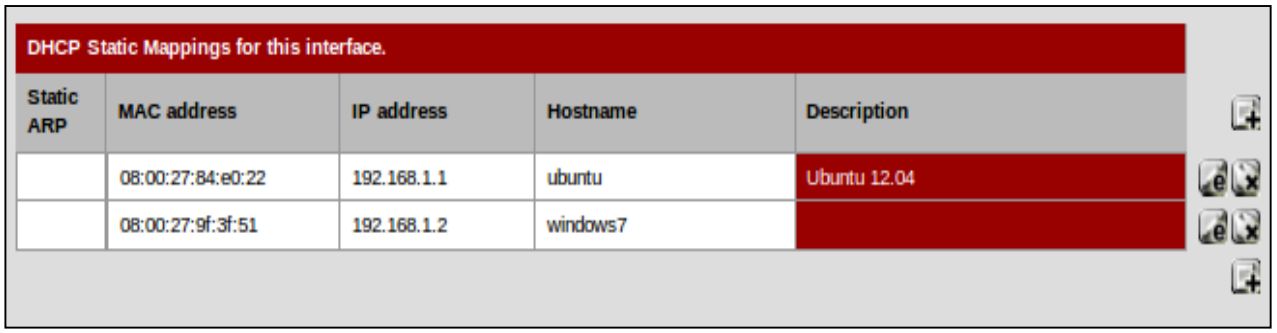
Figura 11 – Configurando IPs rede interna



Fonte: NEVES et al,. (2014)

Se algum host necessitar de receber sempre o mesmo endereço de IP. Ele pode receber um endereço fixo através do mapeamento de um endereço IP específico para um determinado endereço físico, como pode ser verificado na Figura 12 (NEVES et al., 2014).

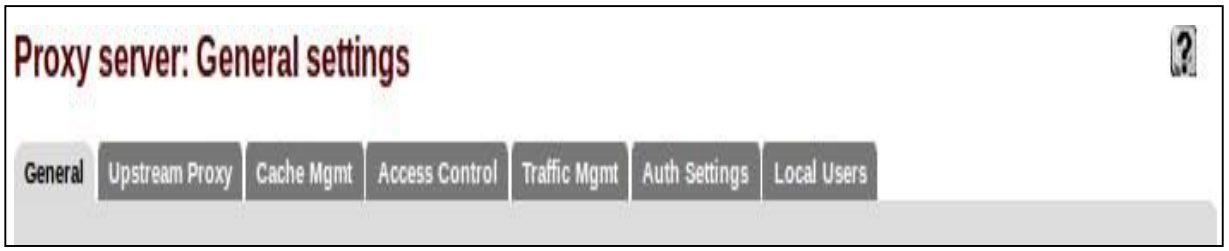
Figura 12 – Mapeamento de IP fixo



Fonte: SABOYA, 2021.

O pfSense juntamente com servidor *proxy*, facilita muito o gerenciamento das configurações. O servidor *proxy* utilizado por este *firewall* é o *squid*, um servidor *proxy* de código aberto utilizado por diversas empresas. Para sua operação é necessário adicionar o pacote através da aba de configurações. Depois de instalado, o servidor fica habilitado para operar, podendo ser configurado na aba de serviços de rede e possuirá as mesmas funcionalidades de um *squid* configurado diretamente em um sistema operacional Linux ou Unix, Como apresentado na Figura 13, há diversas abas de configuração para o servidor *proxy* (NEVES et al., 2014).

Figura 13 – Abas de configuração.



Fonte: NEVES et al,. 2014.

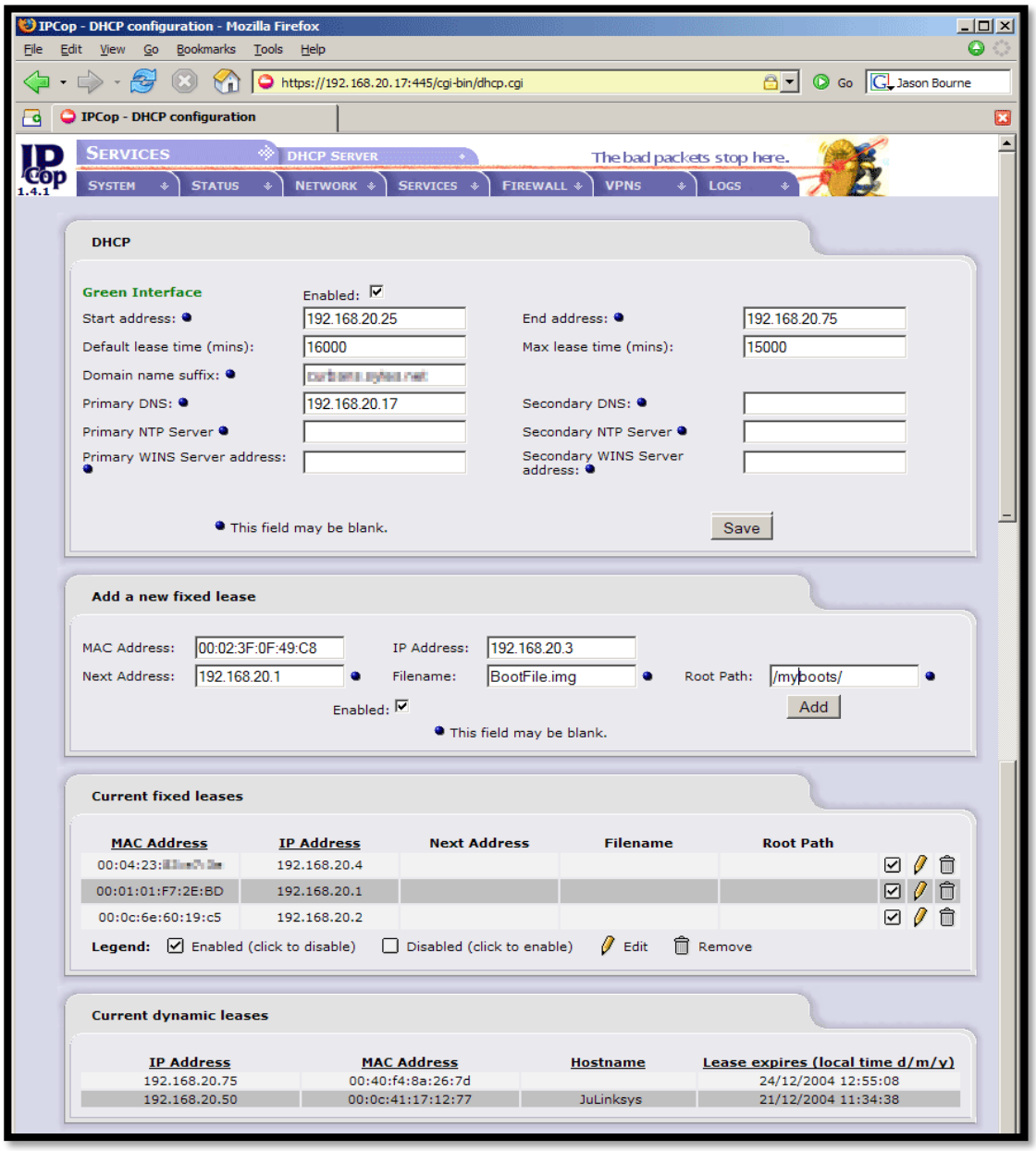
4.3 Visão geral do *Software Endian Firewall*

Endian Firewall é uma distribuição Linux, especializada em roteamento e *firewall.* É um projeto *open source*, baseado no conhecido IPCop, desenvolvido pela

ENDIAN, empresa italiana de gerenciamento e segurança de redes (LIMA, 2017).

O IPCop é uma distribuição Linux que possui como principal foco a proteção de redes de pequeno a médio porte, fazendo isso de maneira facilitada através de uma interface WEB muito intuitiva e funcional, mostrada na Figura 14 (MENEGUITE, 2022).

Figura 14 - Interface WEB IPcop



Fonte: IPCop, 2022.

Endian Firewall Community (EFW) é um produto de *Software* de segurança baseado em Linux, projetado para uso doméstico. Pode transformar um simples *hardware* não utilizado em uma solução de Gerenciamento Unificado de Ameaças (UTM) com todos os recursos. A Comunidade *Endian* foi projetada para simplificar a segurança e ajudar a proteger as redes domésticas usando o poder do *Open Source* (*ENDIAN* SRL, 2022).

Os suíte de recursos do *Endian* incluem *Firewall* de *stateful firewall*, proxies para vários protocolos como HTTP, *Post Office Protocol* (POP3) ou Protocolo dos Correios, *File Transfer Protocol* (FTP) ou Protocolo de Transferência de Arquivos, *Simple Mail Transfer Protocol* (SMTP) ou Protocolo de Transferência de Correio Simples, com suporte antivírus e filtragem de spam para tráfego de e-mail e solução VPN (baseado em *OpenVPN* e IPsec) (TREINAR, 2022).

Por tratar-se de uma distribuição baseada em Linux, o *Endian* atrai usuários que já possuam alguma familiaridade com segurança de sistemas Linux. Além disso, a solução conta com tecnologias integradas pertencentes a outras empresas de segurança, tais como a Panda (responsável pelo motor do Antivírus nativo do *Endian*), a Cyren (líder em soluções de segurança para Internet e e-mail), a Cloud4Wi (desenvolvedor de soluções para redes sem fio comerciais), além de utilizar ferramentas livres e consolidadas como Squid, uma solução de *proxy* bem difundida no mercado (AZEVEDO, 2019).

Endian é um produto planejado e projetado para ajudar os usuários a proteger facilmente suas redes domésticas e não se destina ao uso em redes de produção ou comerciais. *Endian Firewall* inclui um conjunto básico de recursos de segurança para a rede, incluindo um *firewall* de pacote com estado, segurança básica da WEB e de e-mail, antivírus de código aberto e Rede Virtual Privada ou V*irtual Private Network* (VPN), Internet *Protocol Security* (IPsec) e *Secure Sockets Layer* (SSL) (*ENDIAN* SRL, 2022).

O *Endian* é disponibilizado de quatro formas: *Hardware Appliance, Virtual Appliance, Software Appliance* e *Community Appliance*. As versões *Software* e *Community* são solução de UTM em *Software* capaz de ser instalada em um *hardware* simples, transformando-o em um UTM completo. A versão *Community* é similar à versão *Software*, porém sem o suporte comercial e sem custos de aquisição, sendo a plataforma ideal para ser a porta de entrada para as soluções *Endian* (RIBEIRO, 2019).

4.3.1 Requisitos do *Endian firewall*

Os requisitos de um sistema para executar *Endian Firewall* varia dependendo do tamanho da sua rede. Redes com até 25 usuários e cinco conexões VPN precisam de um processador de 1 GHz Pentium III.

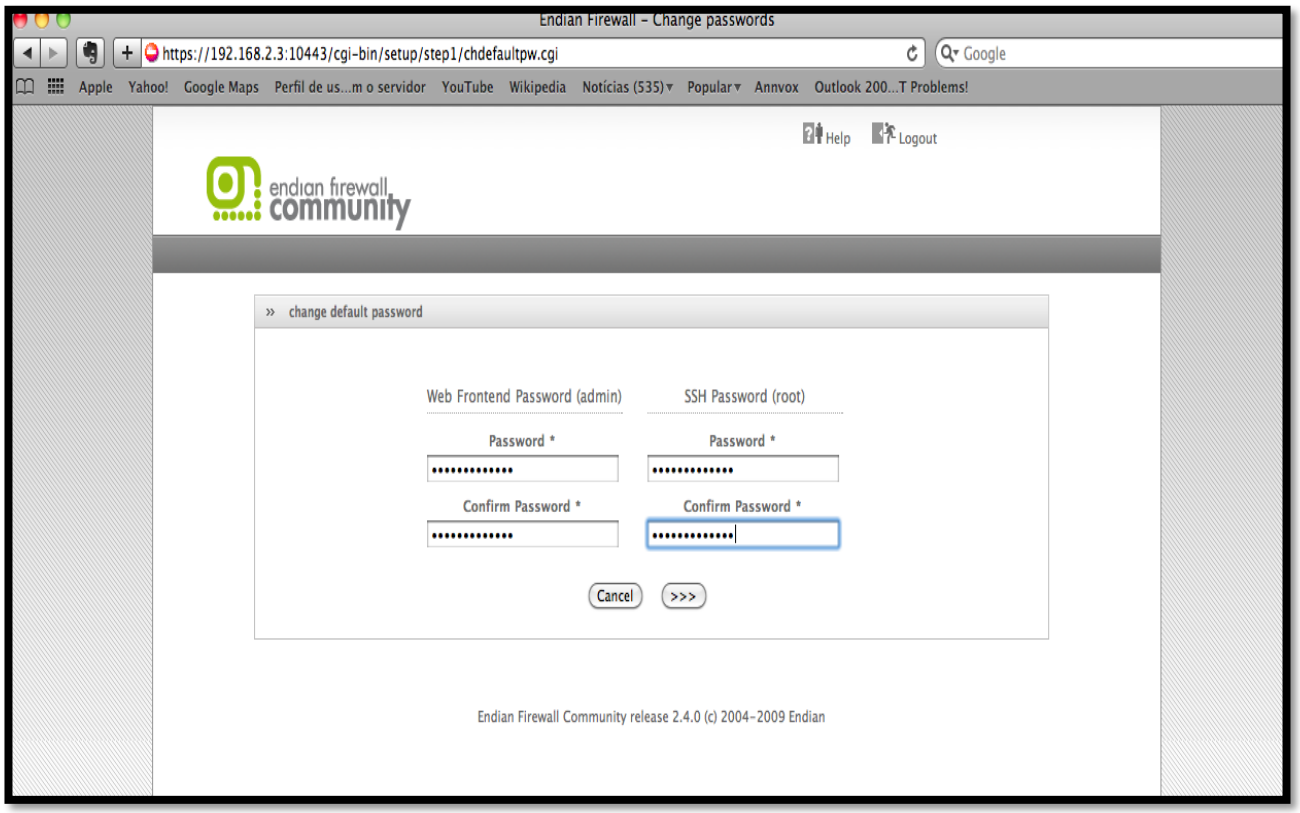
PCs com *Endian Firewall* em redes com até 50 usuários exigem um Pentium IV rodando a 2.8 GHz ou mais rápido.

Para redes um pouco menores basta 512 MB de RAM. Espaço no disco rígido para pequenas redes precisa de pelo menos 8 Giga Bytes (GB) de espaço livre. Já nas redes maiores é necessário 20 GB ou mais. Todos os PCs com *Endian Firewall* precisam de pelo menos duas placas de rede de 100 MB.

Além disso, os computadores com *Endian* devem ser equipados com componentes de resfriamento extra porque eles devem ser executados sem interrupção e podem sobreaquecer (COP e DIREITA, 2022).

A tela inicial do *Endian Firewall*, no primeiro acesso pode ser definido a senha do usuario Admin. Esse usuário será usado para acessar a interface WEB como ilustrado no Figura 15 (HERNANE, 2011).

Figura 15 – Interface WEB *Endian Firewall*



Fonte: DICAS E TUTORIAIS, 2020

A mesma coisa pode ser feita para o usuario *root*, usado para se conectar via *Secure Socket Shell* ou Shell de soquete seguro (SSH).

4.4 Instalação do *Endian Firewall*

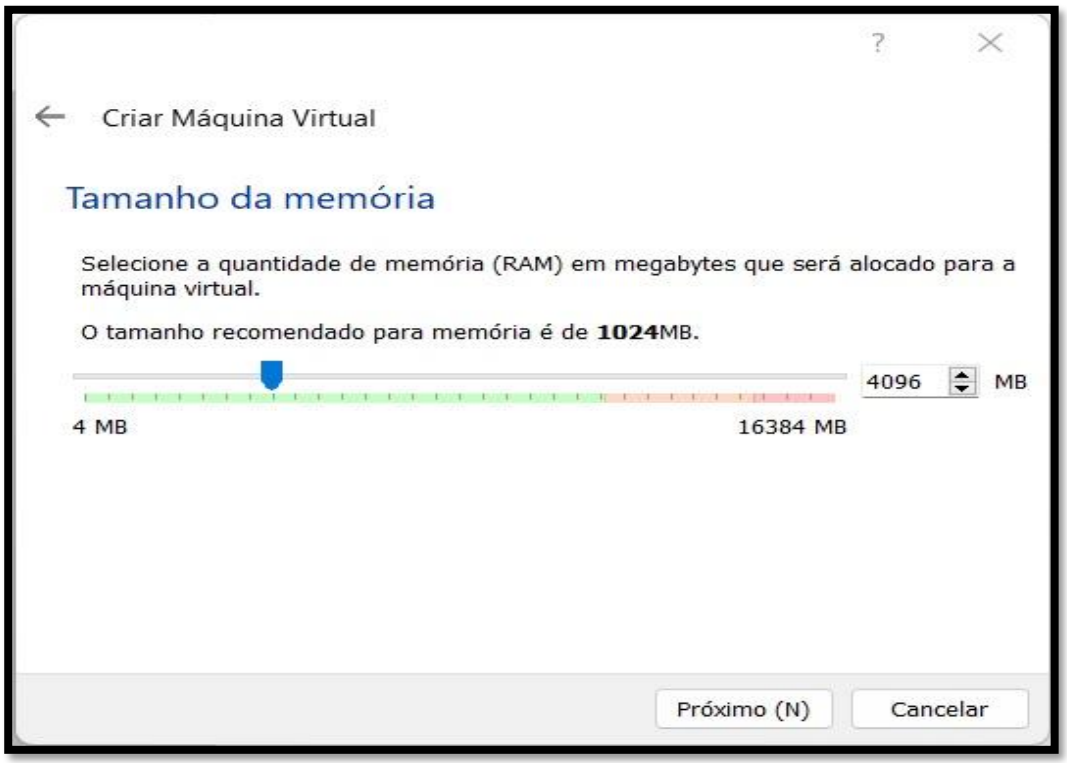
A instalação do *Endian Firewall* foi realizada da seguinte maneira:

Primeiramente foi baixada a imagem ISO do *Endian Firewall* e depois foi configurado um servidor linux no qual foi instalado o *firewall*.

Um arquivo ISO é uma cópia idêntica (imagem) de arquivos gravados num CD, DVD ou BD. Essas imagens são compostas pelo conteúdo total dos dados contidos num disco óptico, incluindo sistema de boot, número de setores gravados, sistema operacional e sistema de arquivos.

Na Figura 16 pode-se observar a quantidade de memoria random access memory (RAM) que foi alocada.

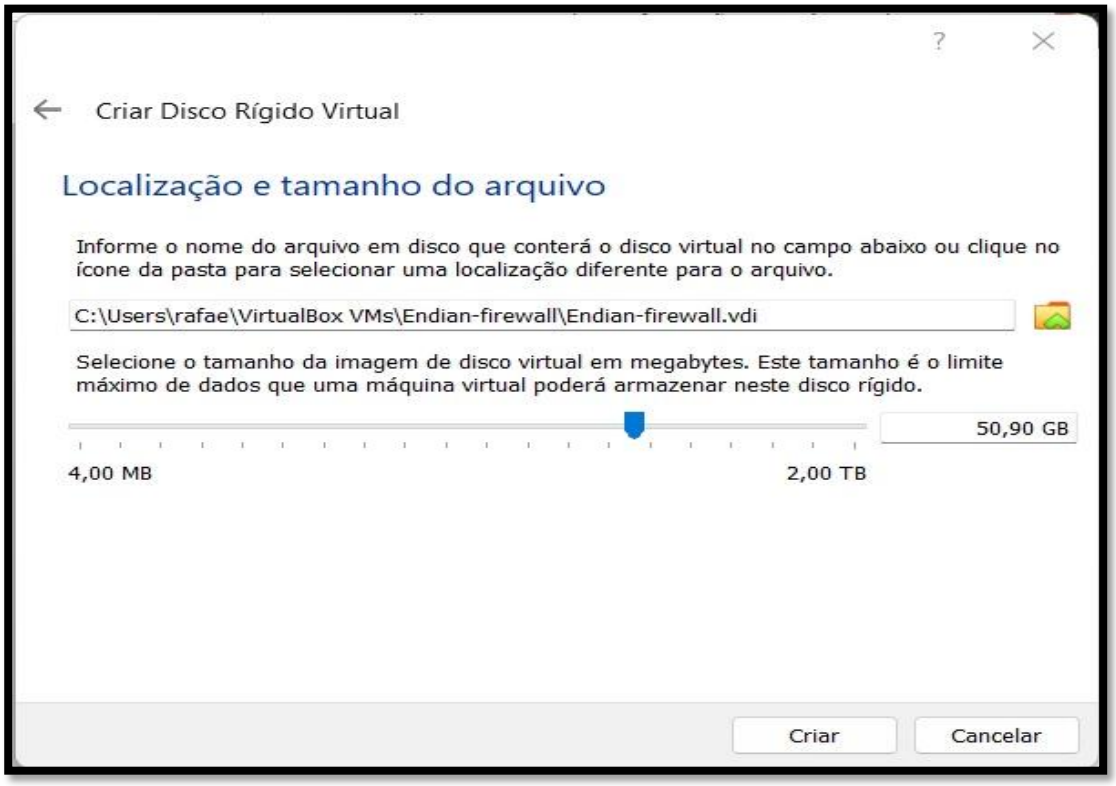
Figura 16 – Memoria RAM Alocada *Endian*



Fonte: Autoria Própria, 2022

Já na Figura 17 mostra a quantidade de memória que foi alocada no disco para as configurações do *Endian*.

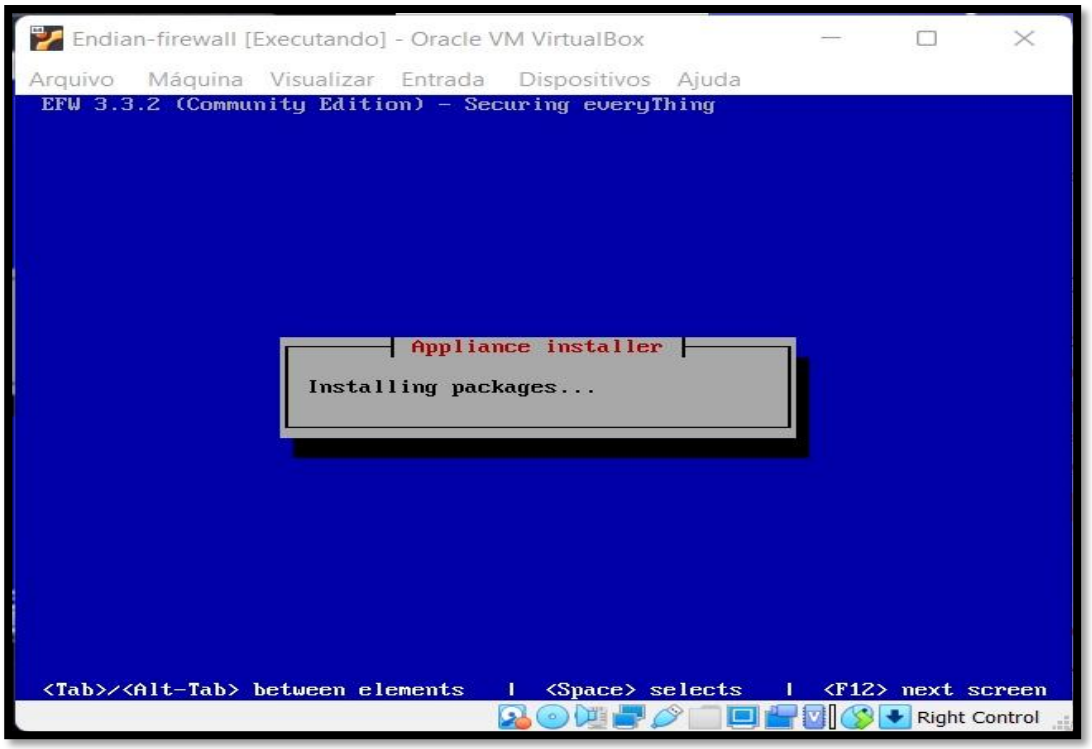
Figura 17 – Memoria no Disco Alocada



Fonte: Autoria Própria, 2022

Depois de configurar o servidor, o sistema foi iniciado. O *Endian* aceita três tipos de idiomas sendo eles o inglês, alemão e italiano. Foi escolhido o idioma inglês. Daí o sistema começou a particionar o disco e, em seguida foram instalados os pacotes pendentes como apresentado na Figura 18.

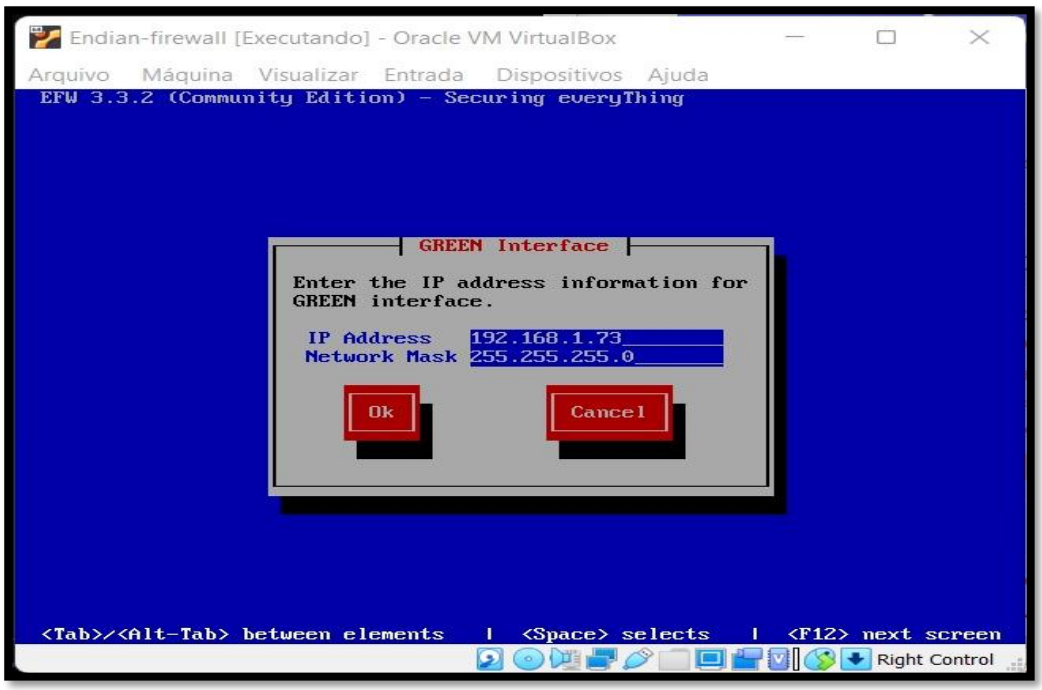
Figura 18 – Instalação dos Pacotes



Fonte: Autoria Própria, 2022

Concluindo a parte de instalação dos arquivos, a Figura 19 mostra a parte onde foi configurada a interface verde, que é a responsável pelo gerenciamento da rede LAN, ou seja, da rede interna da empresa.

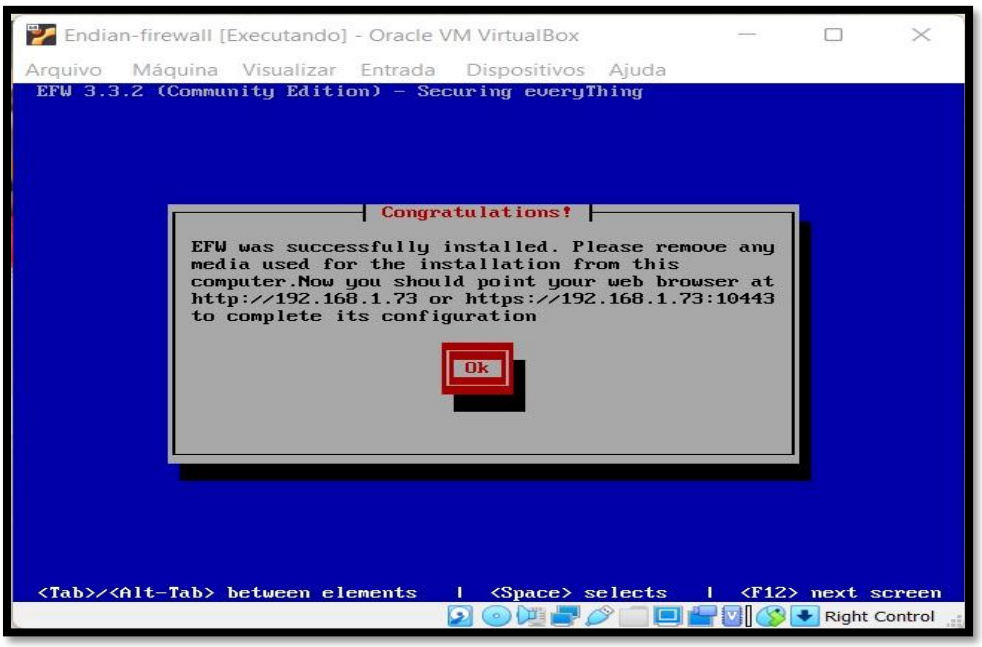
Figura 19 – Interface da Rede interna



Fonte: Autoria Própria, 2022

Quando a instalação foi finalizada o sistema mostrou o IP e porta para a conexão WEB. Realizando este processo, observa-se que não é complexa a instalação do *Endian* e suas configurações ficam mais fáceis de serem executadas, como apresentado na Figura 20.

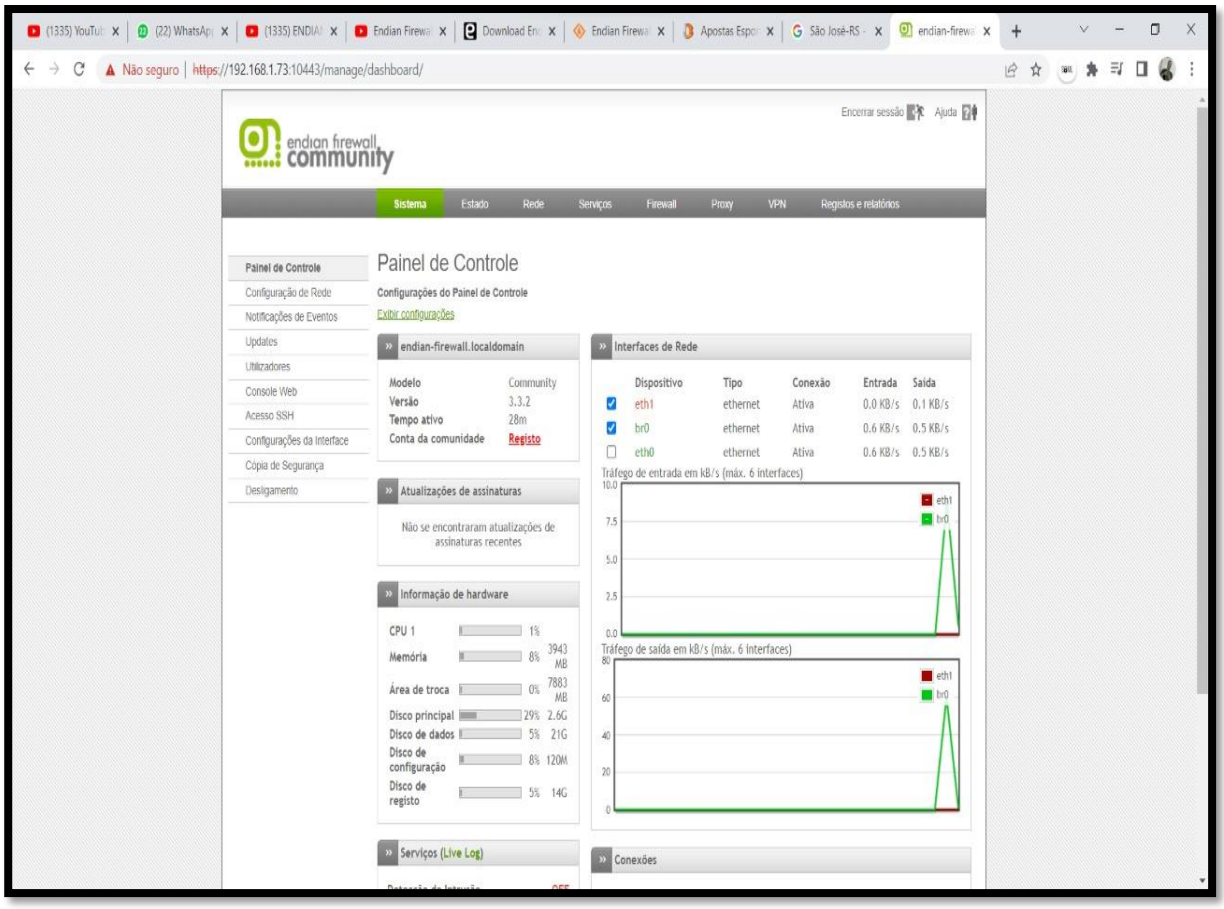
Figura 20 – IP e Porta para Conexão



Fonte: Autoria Própria, 2022

Depois de criar a senha para o admin e a senha para o usuário root do sistema, precisa fazer as configurações básicas de rede que o próprio sistema indica como fazer. Após configurado o sistema exibe a sua interface WEB na qual ficam todas suas funcionalidade, como apresentado na Figura 21.

Figura 21 – Interface Web

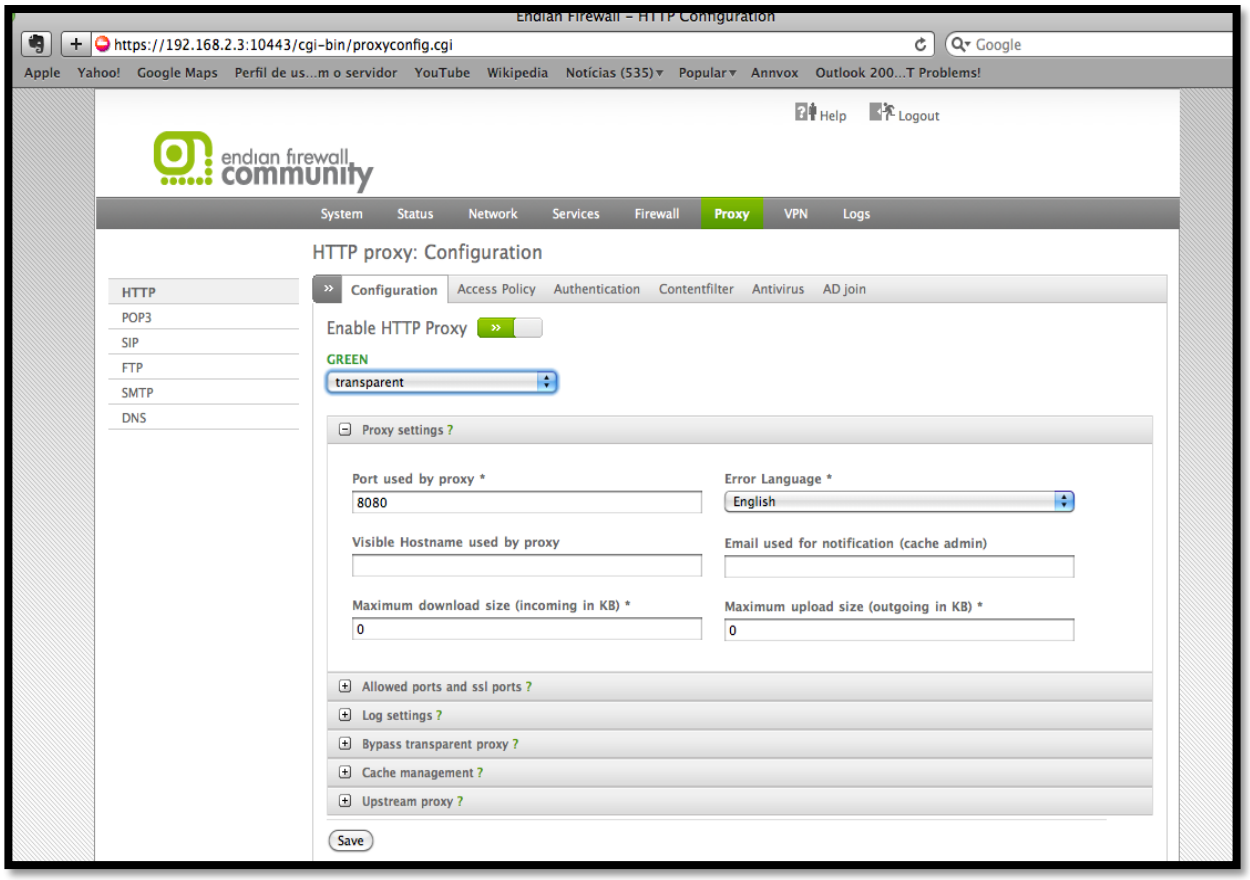


Fonte: Autoria Própria, 2022

O sistema de *Proxy* do *Endian Firewall* é implementado pelo *Software Squid*, para controle de conteúdo. A filtragem de conteúdo pode basear-se em sistema de detecção de palavras específicas, lista de URL's ou endereços IP, podendo estabelecer horários para bloqueio ou liberação.

Na aba *Proxy* pode-se ver e configurar nosso *Proxy*. na Figura 22 foi habilitado o HTTP *Proxy* e depois foi colocada a opção transparente. Assim, todas as solicitações podem ser automaticamente redirecionandas para o *Proxy* (HERNANE, 2011).

Figura 22 – Habilitando HTTP *Proxy*



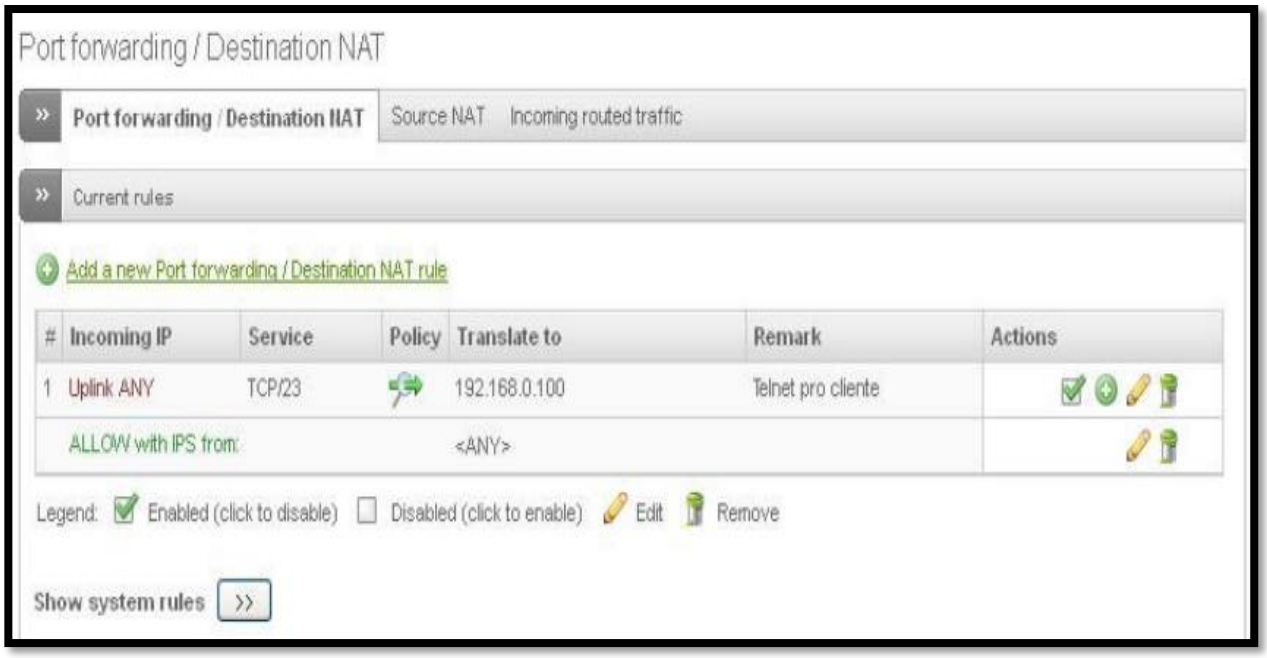
Fonte: DICAS E TUTORIAS, 2020

Na Figura 22 foi escolhida a opção transparente, ou seja, não exige configurações do *Software* cliente WEB para acessar o servidor.

O *Endian Firewall* fornece uma interface WEB simples para configuração de regras do *firewall iptables*. Para tal, o administrador da rede deve clicar em *firewall* no menu superior.

O administrador pode configurar um encaminhamento de portas, permitindo que conexões externas sejam redirecionadas para algum computador da rede interna, selecionando no menu esquerdo a opção "*Port forwarding* / *Destination* NAT, obtendo a tela mostrada na Figura 23 (RAIMUNDO et al., 2011).

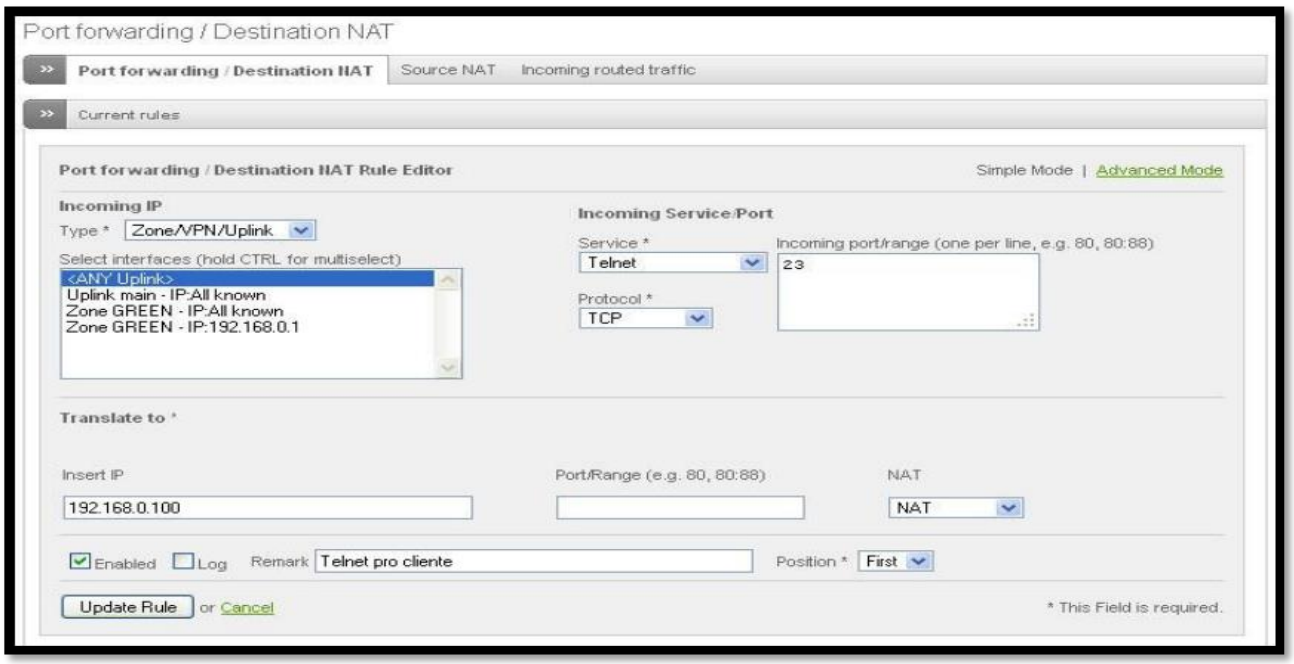
Figura 23- Encaminhamento de porta



Fonte: FDOCUMENTOS, 2018

Clicando em "*Add a new Port forwarding/Destination NAT rule*", o administrador da rede pode configurar as requisições o serviço ou portas associadas e o endereço ao qual a requisição será redirecionada, como mostrado na Figura 24 (RAIMUNDO et al., 2011)

Figura 24 - Adicionando um Encaminhamento de Porta



Fonte: FDOCUMENTOS, 2018

5 Kali Linux

O kali Linux e uma distribuição Linux baseada no Debian. Criada em 2013 ela e um sucessor do BackTrac. O Kali Linux é uma poderosa distribuição focada em ferramentas de invasão, Ele tem o intuito de auxiliar os profissionais de segurança da informação. A distribuição tem uma grande variedade de ferramentas ao total são mais de 300, exclusivas para pentests e atividade de segurança (BRITO, 2021).

O kali Linux é uma das poucas distribuições Linux com foco em hackers, O Kali dispõe de numerosos *Softwares* pré-instalados, incluindo o Nmap (*port scanner*), *Wireshark* (um *sniffer*), *John the Ripper* (crackeador de senha) e *Aircrack-ng* (*Software* para testes de segurança em redes sem fios) (PROGRAMADORES, 2020).

Network Mapper (NMap) ou mapeamento de rede trata-se de uma ferramenta de código aberto para exploração de rede e auditoria de segurança. O Nmap foi projetado para escanear, rapidamente, grandes redes. A ferramenta usa pacotes IP brutos de maneiras inovadoras para determinar quais hosts estão disponíveis na rede, quais serviços esses hosts estão oferecendo, quais sistemas operacionais eles estão executando, que tipo de filtros/*Firewall*s de pacotes estão em uso e dezenas de outras características (DIOLINUX, 2021).

O *Wireshark* é um programa que analisa o tráfego de rede e o organiza por protocolos. Através dessa aplicação é possível controlar o tráfego de uma rede e monitorar a entrada e saída de dados do computador, em diferentes protocolos, ou da rede na qual o computador está ligado. Também é possível controlar o tráfego de um determinado dispositivo de rede numa máquina que pode ter um ou mais desses dispositivos (PETTERS, 2020).

John the Ripper (JtR) é uma das ferramentas de *hacking* mais populares que existe para quebrar senhas. O JtR detecta automaticamente a criptografia nos dados com hash e a compara com um grande arquivo de texto simples que contém senhas populares, criptografando cada senha e interrompendo quando encontra uma correspondência (PROFISSIONAIS TI, 2020).

O *Aircrack-ng* é um conjunto completo de ferramentas para avaliar a segurança da rede *WiFi*. Ele se concentra em diferentes áreas de segurança *WiFi* como: monitoramento, ataque, teste e cracking. Funciona com qualquer placa *wireless* cujo driver suporta modo de monitoramento bruto, podendo capturar e

analisar os dados da rede (MACEDO, 2016).

5.1 Requisitos minimos para instalação do Kali Linux:

Para se instalar este *Software* é preciso uma maquina com a seguinte configuração:

- 8 GB de espaço em disco para a instalação.
- No mínimo 512MB de RAM para as arquiteturas i386 e amd64.
- Suporte a boot pelo drive de CD-DVD / *Universal Serial Bus* (USB)
- Suporte a instalações via *VirtuaBox / Wmware Player*
- Tamanho da imagem .ISO – 2.6Gb Plataformas: 32 e 64 bits

Toda sua instalação está detalhada no Apêndice A

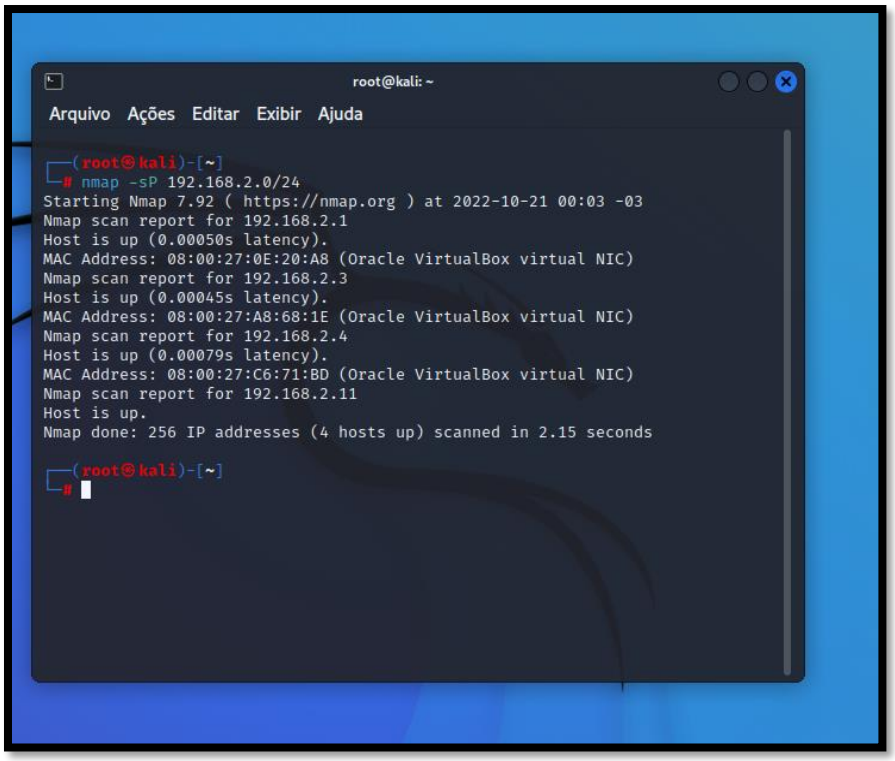
5.2 Experimentos: Ataque do tipo Nmap

Para realização do experimento foi necessário instalar duas maquinas virtuais ou *virtual machine* (VMs). Para montar o laboratório foram colocados os 2 servidores na mesma rede em que o Endian faz o controle. Usando o servidor de DHCP do endian ficou fácil de atribuir IPs para cada maquina. Foi colocada na mesma rede um hacker de nossa autoria, para facilitar os experimentos, ou seja, os ataques.

No inicio do ataque, o Kally linux fez uma *Ping Sweep*, também chamada de varredura de protocolo de mensagem de controle da Internet ou *Internet Control Message Protocol* (ICMP), que é uma técnica de diagnóstico usada na computação para ver qual intervalo de endereços IPs está em uso por hosts ativos, que geralmente são computadores.

Esta varredura é geralmente usada para informar quais as máquinas ativas estão em uma rede, conforme ilustra a Figura 25.

Figura 25 – Identificação de Hosts na Rede, usando *Ping Sweep*

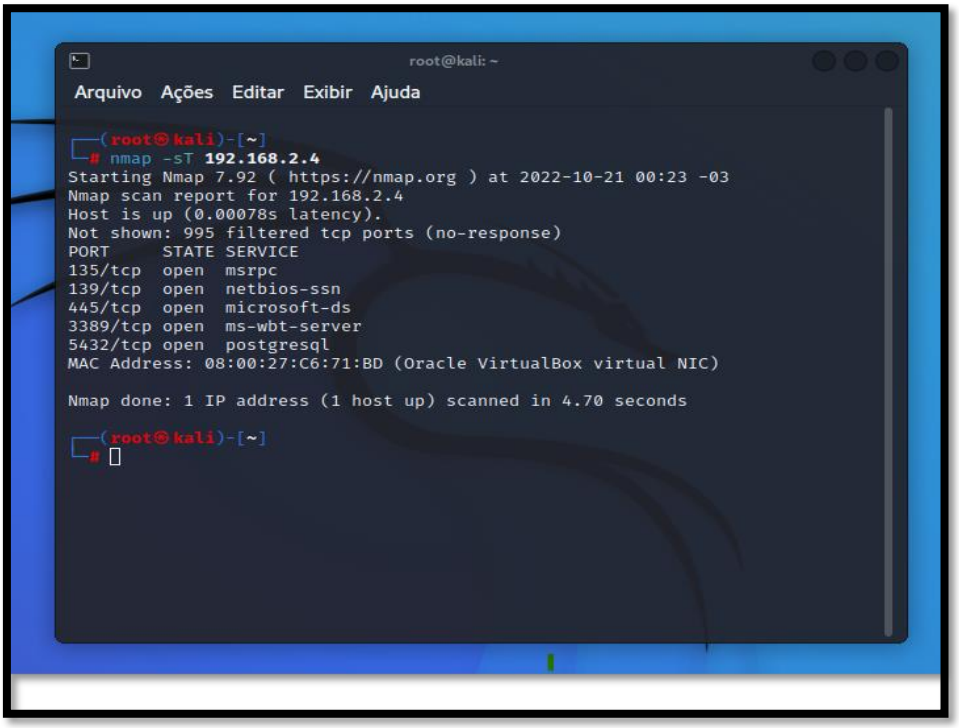


Fonte: Autoria Própria, 2022

Com o comando "IP a" no terminal do Linux ou ipconfig no Prompt de Comando (CMD) do windowns pode-se ver em qual rede esta maquina. Como pode ser visto na Figura 25, executando o comando nmap -sP 192.168.2.0/24, são mostrados todos os dispositivos conectados nesta rede. Este endereço IP colocado no comando precisaser o endereço IP de rede. Primeiro, é trazido em primeiro lugar o gateway padrão (192.168.2.1), depois em ordem crescente, são listados todos os hosts que estão ativos na rede.

Suponha que a maquina de interesse será a de endereço 192.168.2.4, iniciando com ataque de *port-scan*. Conforme pode ser visto na Figura 26, executando o comando nmap -sT 192.168.2.4, é feita uma varredura e traz todas as portas abertas do servidor. Nesse exemplo, pode ser visto que nesse servidor existe um banco de dados instalado, e está usando sua porta padrão que é o famoso Postgres na porta 5432/tcp.

Figura 26 – Portas abertas no servidor



Fonte: Autoria Própria, 2022

O ataque Nmap foi escolhido pois é muito usado por hackers devido a sua facilidade de fazer varreduras em sistemas. Depois de fazer um varredura na rede do laboratório, o ataque teve sucesso em obter todas os host conectados na rede. Depois de escolher um host para simular o ataque, passando o parâmetro -sT foi feito um port scan do tipo TCP na maquina selecionada, na qual o Nmap conseguiu trazer todas as portas abertas.

6 FUNCIONALIDADES DO *ENDIAN FIREWALL*

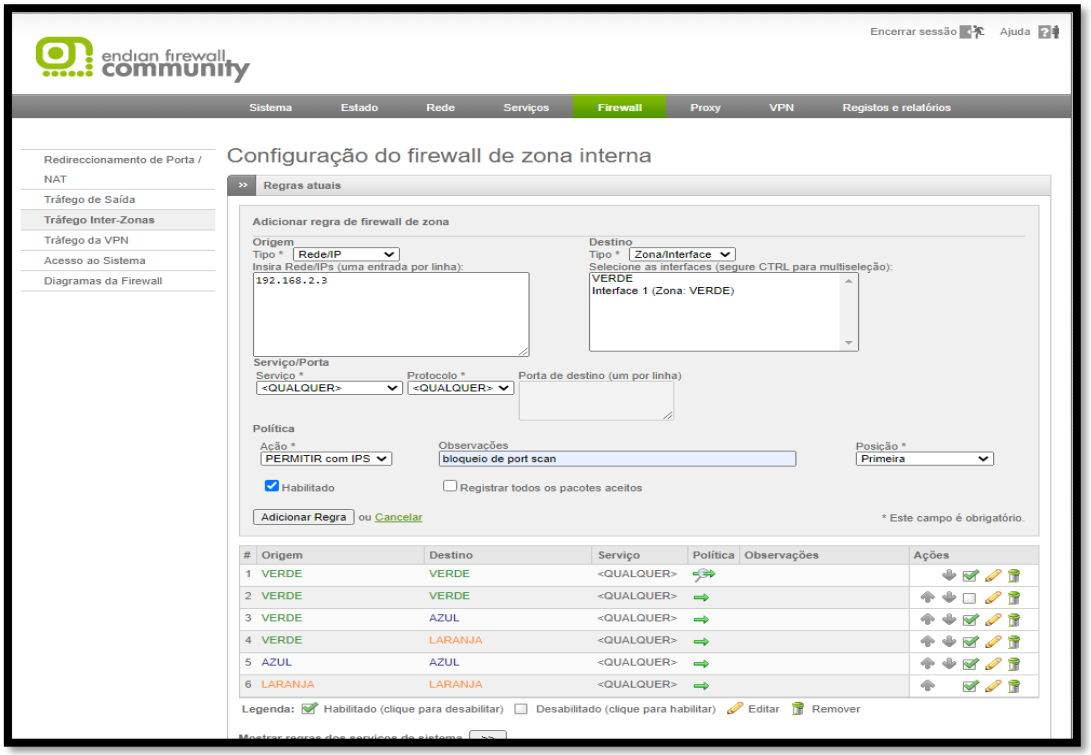
Nesse capitulo serão descritas as funcionalidades e como foram realizadas as configurações do *Endian Firewall.*

6.1 Sistema de Prevenção de Intrusão ou *Intrusion Prevention System* (IPS)

Para conseguir enibir o ataque de *port scan* do *Nmap* é preciso ativar a funcionalidade (IPS), clicando na aba “serviços”. Depois no menu lateral esquerdo “prevenção a intrusão”, e assim, a funcionalidade será habilitada. Para configurar o bloqueio clica na aba “*firewall” e* depois em trafego “enter-zonas”. Depois clicar em adicionar uma nova regra de firewall**.** Foi configurado o IP de origem 192.168.2.3 e no destino foi configurado toda a zona verde, que é a rede administrada pela Endian. Os serviços e protocolos foram atribuidos “qualquer” que corresponde todos os tipos de serviços e portas.

Como pode ser visto na Figura 27, a regra foi colocada em primeiro lugar na lista de regras e na politica de acesso foi colocado “PERMITIR com IPS”. Para finalizar a configuração da regra clica-se em adicinar regra e aplicar.

Figura 27 – PERMITIR com IPS



Fonte: Autoria Própria, 2022

A politica de acesso PERMITIR com IPS consegue previnir o *port scan*, pois o ataque do NMAP funciona com tentativas de conexão**.** Ele manda as requisições para todas as portas e, quando a porta responder, ele consegue indentificar que esta porta está aberta. Daí é informado um relatório no NMAP com todas as portas que estão abertas. Quando o *port scan* começa a rodar, o Endian percebe as várias tentativas de conexões (ataques) e, então bloqueia as mesmas, através da regra do Firewall (IPS).

6.2 Servidor DHCP

Na aba serviços, clicando no Servidor DHCP, em seguida, em ativar o serviço na interface verde e abrir a configurações, podem ser vistas todas as configurações deste servidor. Na Figura 28 mostra como foi configurado. O endereço inicial de IP é 192.168.2.2 e o final 192.168.2.50. Assim, o servidor DHCP poderá distribuir um total de 48 endereços IPs pela rede.

Figura 28 – Quantidades de IPs

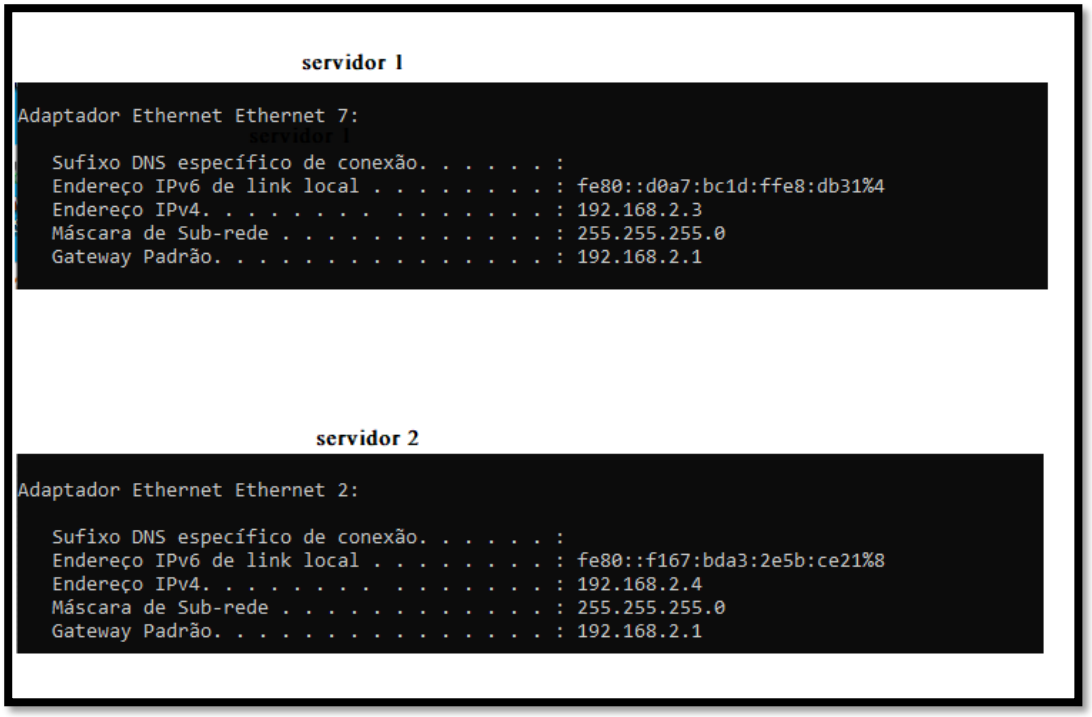
Fonte: Autoria Própria, 2022

Como pode ser visto na Figura 28, o endereço IP inicial para os hosts é 192.168.2.2, pois 192.168.2.0 é destinado àrede e o 192.168.2.1 é destinado ao

Gateway padrão. No DNS secundário foi configurado o IP do google 8.8.8.8.

Iniciando os 2 servidores depois de aplicar as configurações do servidor DHCP, o Endian atribui um IP para cada maquina. Usando o endereço MAC do servidor para diferenciar cada maquina, o primeiro servidor recebe o endereço IP dinâmico 192.168.2.3. O segundo servidor recebe o endereço 192.168.2.4, como pode ser visto na Figura 31.

Figura 29 – IPs Destribuidos pelo DNS



Fonte: Autoria Própria, 2022

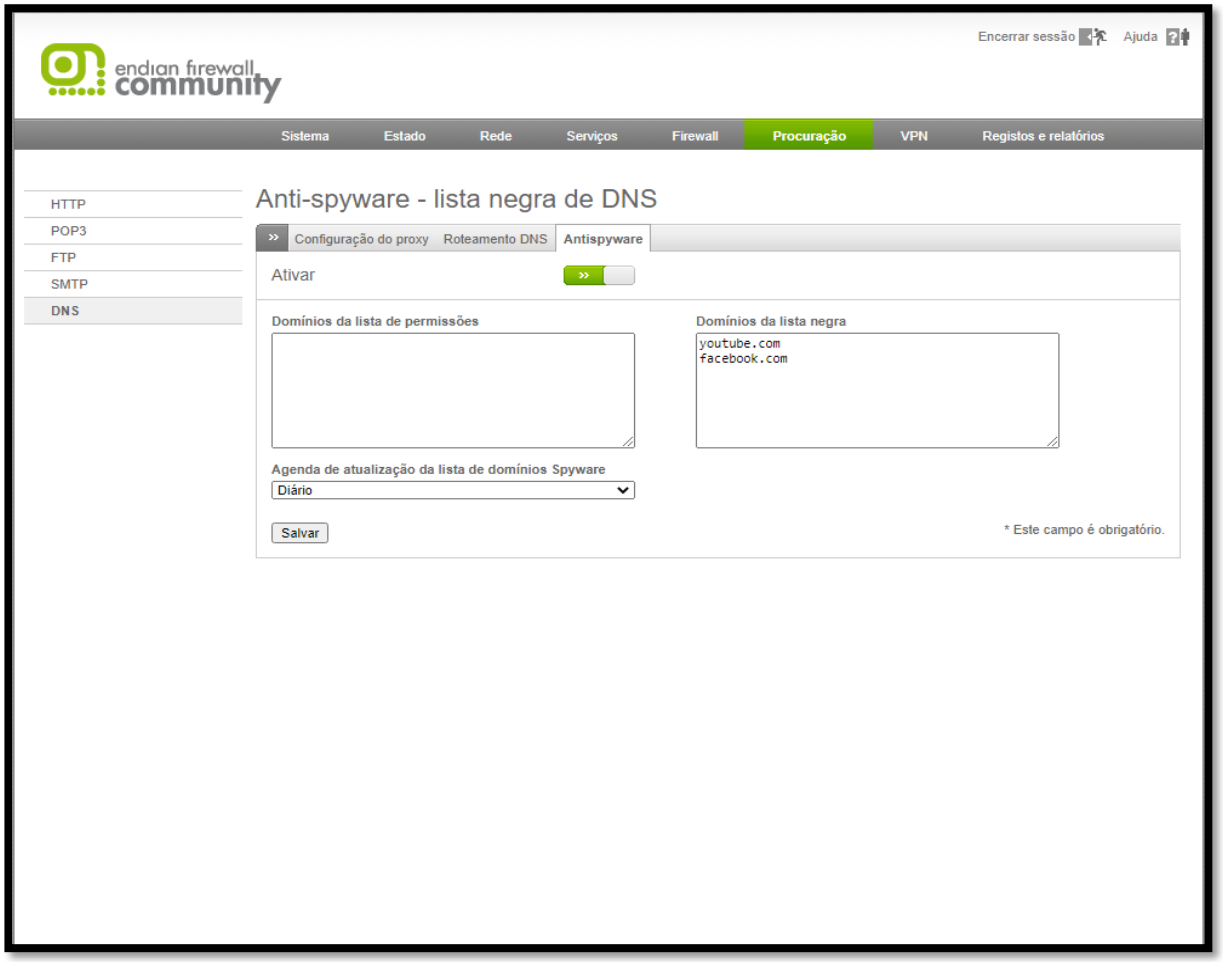
6.2 Proxy- Bloqueios de Dominios

O Proxy é uma funcionalidade muito importante para que os administradores da rede tenham o controle sobre os sites e domínios que os usuários estão acessando. Para configurar os bloqueios primeiro clica na aba *proxy* , em seguida no menu lateral esquerdo DNS, depois em *Anti-spyware* e ativar. De um lado tem-se a lista de domínios com permissões de acesso. Do outro lado vão ser ser inseridos os domínios e subdomínios que serão bloqueados pelo administrador da rede.

Como pode ser visto na Figura 30 os testes foram feitos em dois sites: o youtube.com e o facebook.com. Observa-se que não foi colocado o ".br "no final, pois

assim o *Endian Firewall* consegue bloquear por completo todos os subdomínios.

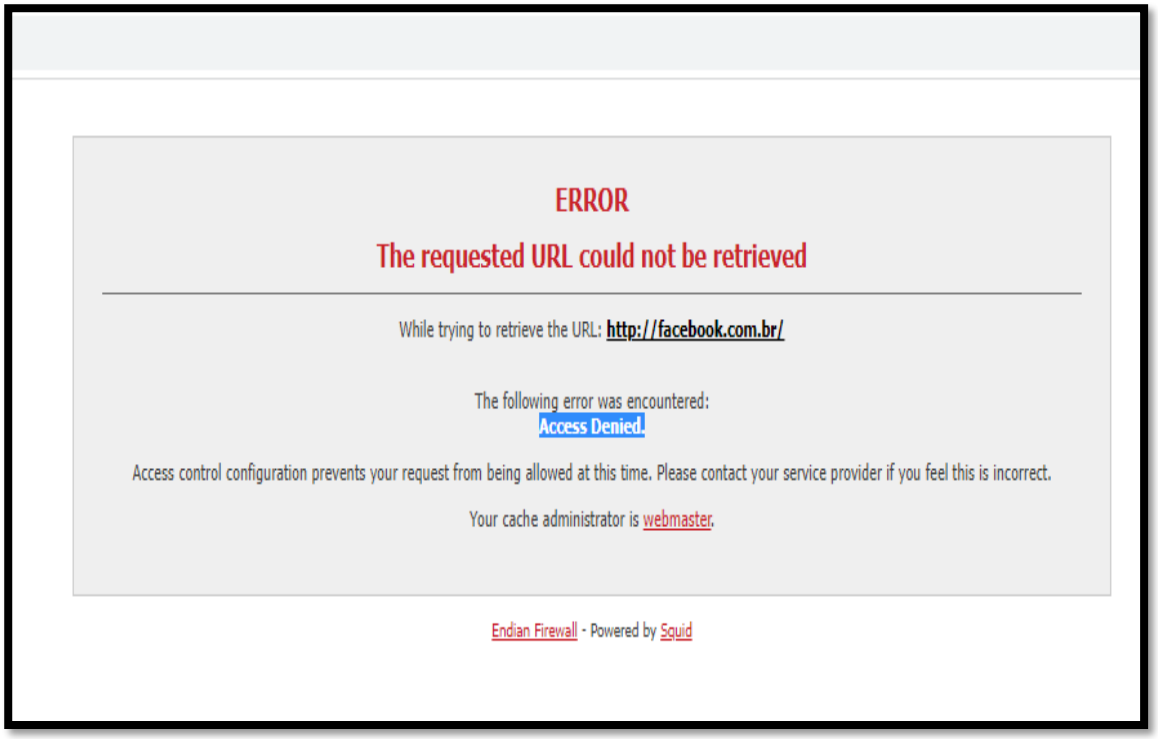
Figura 30 – Dominios Bloqueados



Fonte: Autoria Própria, 2022

Ao tentar acessar a pagina fecebook.com.br o usuário receberá a seguinte mensagem: "*Access Denied*" ou Acesso negado, como ilustrado na Figura 31 .

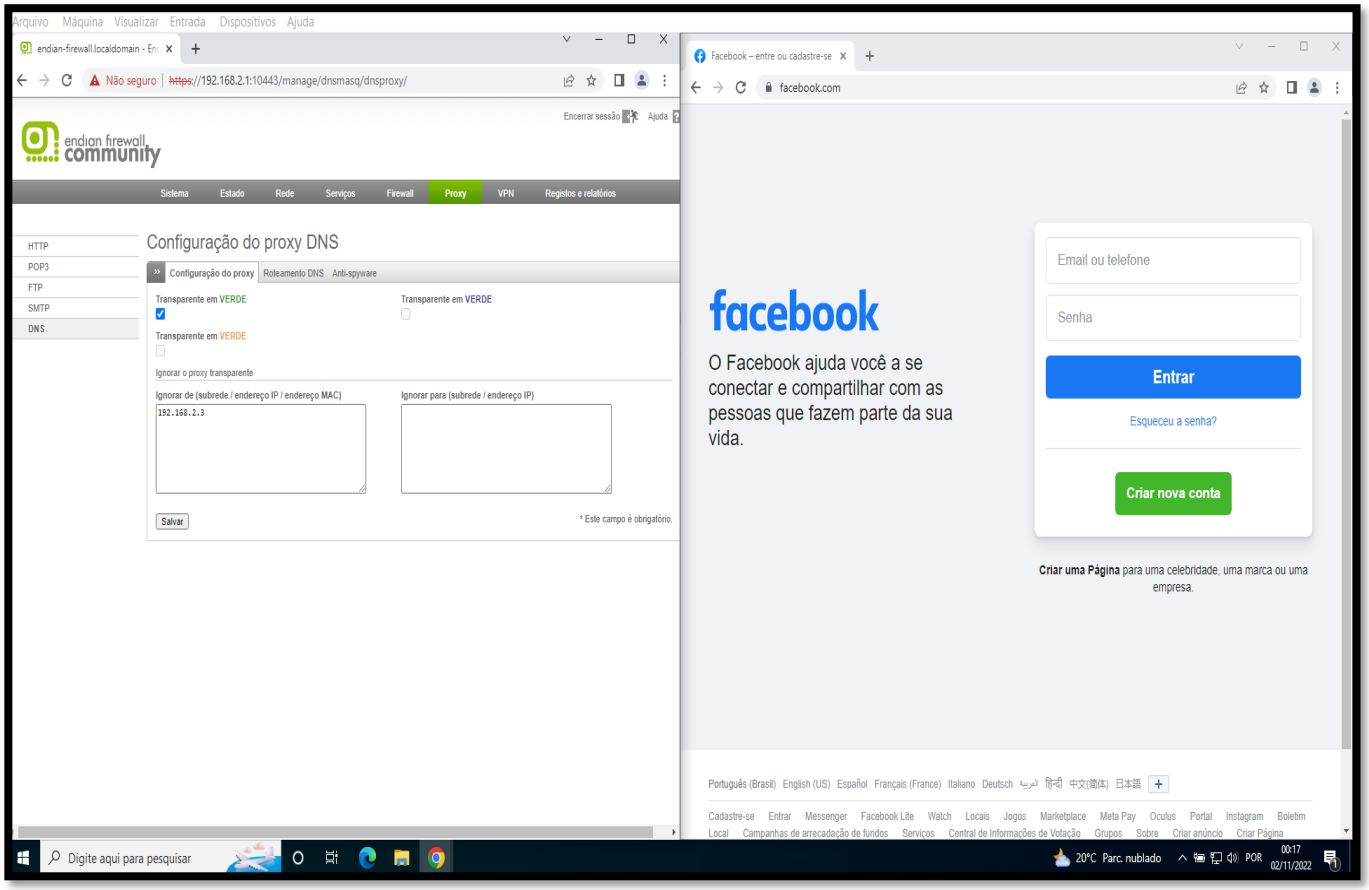
Figura 31 – Mensagem de Acesso Negado



Fonte: Autoria Própria, 2022

Se algum usuário precisar de usar algum dos sites bloqueados pelo administrador da rede, ele terá que solicitar a liberação. O administrado da rede vai liberar o acesso usando a seguinte configuração vista na Figura 32. Existe uma configuração “ignorar o *proxy* transparente”. Como seu próprio nome indica, pode ser colocado o endereço MAC, subrede ou endereço IP de um host. Assim, o servidor vai ignorar os bloqueios feitos pelo proxy do Endian.

Figura 32 – Acesso Liberado pelo IP do host



Fonte: Autoria Própria, 2022

Este teste, na pratica, foi realizado com o servidor 1, colocando seu endereço 192.168.2.3 . Assim, o acesso foi liberado porque o host ignorou as configuração do proxy.

7 CONCLUSÕES

Este trabalho buscou responder a seguinte questão de pesquisa: **- Quais as funcionalidades dos *firewall Pfsense e Endian* para segurança das redes de computadores?**

O objetivo geral foi o de **i**dentificar e descrever as funcionalidades dos *firewall Pfsense e Endian,* usados em redes de computadores. Entretanto, este estudo focou mais no *Endian Firewall*, por este ser menos explorado na literatura.

O estudo permitiu identificar que as funcionalidades mais usadas no *Endian Firewall* são: Sistema de Prevensão de Intrusão, Servidor DCHP, Proxy Bloqueio de domínios e ignorar o proxy transparente.

Observou-se que quando o Nmap é usado por um administrador de rede, esta ferrramenta pode ser muito útil para aumentar a segurança das redes, porque oferece uma forma rápida e eficiente de diagnósticos do sistema, mesmo sendo uma ferramenta usada pelos *hackers*. Além disso, o administrador vendo toda a varredura da sua rede, ele pode identificar e administrar melhor sua própria rede. Assim, conclui-se que o Nmap pode oferecer funcionalidades que complementam a segurança de dados de uma rede de computadores.

Usando o sistema operacional Kalli Linux e a ferramenta Nmap, foi possivel demonstrar que o *Endian Firewall* possui funcionalidades que realmente funcionam para bloquear os ataques ou acessos não permitidos. Assim, foi possivel concluir que o *Endian Firewall* é eficaz e atende aos requisitos para que uma rede de computadores possa ser protegida e organizada. Além disso, é um software amigável e intuituivo, facilitando que qualquer um que tenha um conhecimento mínimo de redes poderá administrar uma rede de computadores residencial ou até uma rede empresarial de pequeno porte.

Assim, este trabalho pode auxiliar um administrador de redes fazer a instalação e as configurações das funcionalidades do Endian Firewal, além do Kalli Linux e do Nmap. Além disso, pode auxiliar qualquer pessoa que deseja manter a sua rede domestica protegida e organizada .

Para continuidade desta pesquisa sugere-se os seguintes trabalhos futuros:

- Realizar mais alguns ataques para testar a eficácia do *Endian Firewall;*
- Pesquisar e descrever mais funcionalidades deste firewall.

8 REFERÊNCIAS BIBLIOGRÁFICAS

BLUE TEAM E RED TEAM: ENTENDA O QUE SÃO E A IMPORTÂNCIA DE CADA UM. **Strong Security**, 2019. Disponível em: < https://www.strongsecurity.com.br/blog/blue-team-e-red-team-entenda-o-que-sao-e-a-importancia-de-cada-um/> . Acesso em: 03, jun. 2022.

BLUE TEAM: COMO ELE PODE ATUAR NAS ESTRATÉGIAS DE CIBERSEGURANÇA DA SUA EMPRESA. **Aser security,** 2022. Disponível em: < https://www.aser.com.br/blue-team-como-ele-pode-atuar-nas-estrategias-de-ciberseguranca-da-sua-empresa/> .Acesso em: 22, jun. 2022.

BLUE TEAM E RED TEAM, ENTENDA O QUE É E QUAIS AS DIFERENÇAS. **Ostec**, 2022. Disponível em: < https://ostec.blog/geral/blue-team-red-team/> . Acesso em: 20, jun. 2022.

BRANDÃO, Guilherme Henrique Freitas. SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS: UM ESTUDO TEÓRICO E EXPERIMENTAL SOBRE AS REDES SOCIAIS.2021. Monografia (Conclusão do curso) - Pontifícia Universidade Católica de Goiás, Escola de Ciências Exatas e da Computação, Gioânia.

BRITO, Edivaldo. Coisas que você deve saber antes de usar o Kali Linux. **Descomplicando Linux,** 2021. Disponível em: < https://www.edivaldobrito.com.br/coisas-que-voce-deve-saber-antes-de-usar-o-kali-linux/> . Acesso em: 15, jun. 2022.

BOFF, Julio Cesar. **Análise das Distribuições Pfsense e *Endian* para Implantação de *Firewall* em Redes Soho.** 2015, Monografia (Conclusão do curso)- Universidade Tecnológica Federal do Paraná. Departamento Acadêmico de Informática Especialização em Redes de Computadores. Disponível em: < http://repositorio.utfpr.edu.br:8080/jspui/bitstream/1/23126/3/PB_ESPRC_II_2015_01.pdf >. Acesso em: 03, maio. 2022.

COMO QUEBRAR SENHAS COM O PROGRAMA JOHN THE RIPPER. **Profissionais TI,** 2020. Disponível em:< https://www.profissionaisti.com.br/como-quebrar-senhas-com-john-the-ripper/> . Acesso em: 03, ago. 2022.

Differbetween, DIFERENÇA ENTRE GPL E LGPL, 2022. Disponível em: < https://pt .differbetween.com/article/difference_between_gpl_and_lgpl>. Acesso em:

14, maio 2022.

Profissionais Linux,FERRAMENTA DE *FIREWALL*., 2022. Disponível em: < https://e-tinet.com/linux/pfsense-vantagens/>. Acesso em: 22, abr. 2022.

FIREWALL PFSENSE. **Sutel**, 2022. Disponível em: < http://www.sutel.com.br /blog/index.php/en/infraestrutura/21-*Firewall*-pfsense>. Acesso em: 24, mar. 2022.

FREE OPEN SOURCE UTM SOLUTION FOR HOME NETWORKS. ***Endian*,** 2022. Disponível em: < https://www.*Endian*.com/de/community/>. Acesso em: 05, abr. 2022

GANHANDO EFICIÊNCIA COM O *FIREWALL* OPEN SOURCE PFSENSE. **Profissionais TI**, 2022. Disponivel em: < https://www.profissionaisti.com.br/ ganhando-eficiencia-com-o-*Firewall*-open-source-pfsense/>. Acesso em : 28, mar. 2022.

INSTALANDO E FAZENDO AS CONFIGURAÇÕES INICIAIS NO *ENDIAN FIREWALL*. **Dicas e Tutorias,** 2020. Disponível em: < https://hernaneac.wordpress .com/2011/03/14/tutorial-instalando-e-fazendo-as-configuracoes-iniciais-no-*Endian-Firewall*/>. Acesso em: 07, maio. 2022.

KALI LINUX: SAIBA TUDO SOBRE ESTA DISTRIBUIÇÃO LINUX. **Programadores,** 2020. Disponível em: < https://programadoresbrasil.com.br/2020/03/kali-linux-download/> . Acesso em: 16, jun. 2022.

LIMA, Fabio Marcelo. *Endian Firewall* - Solução completa para um servidor de internet. **Viva o Linux,** 2017. Disponível em: https://www.vivaolinux.com.br/artigo /*Endian-Firewall*-solucao-completa-para-um-servidor-de-internet. Acesso em: 01, abr. 2022.

LUCENA, Felipe. **Segurança de Dados: tudo que você precisa saber**. Diferencial TI. 2017. Disponível em: <https://blog.diferencialti.com.br/seguranca-

de-dados/ > .Acesso em: 05, mar. 2022.

MACEDO, Diego. **WPA2**, 2022. Disponível em: < https://www.diegomacedo.com.br/author/admin/> .Acesso em: 05, ago. 2022.

MACEDO, Ricardo Tombesi et, al. Redes de Computadores. 1.ed. Rio Grande do Sul, 2018. Disponível em: < https://www.ufsm.br/app/uploads/sites/358/2019/08/MD_RedesdeComputadores.pdf>. Acesso em: 25, abr. 2022.

MACHADO, Bruna Carneiro. As Vulnerabilidades dos Dados e as Formas de Ataques.2021. Monografia (Conclusão do curso) - Pontifícia Universidade Católica de Goiás, Escola de Ciências Exatas e da Computação, Gioânia.

MENEGUITE, Ronaldo. Introdução ao *Firewall* IPCop.**Segurança/infraestrutura,** 2017. Disponível em: < https://meneguite.com/2010/01/15/introducao-ao-*Firewall*-ipcop/> . Acesso em: 05, abr. 2022.

MONQUEIRO, Julio Cesar Bessa. Primeiras impressões do FreeBSD 7.0. ***Hardware*.com.br**, 2018. Disponível em: < https://www.*hardware*.com.br/dicas/freebsd7.html>. Acesso em: 06, abr. 2022.

MOREIRA, C.; BEIRA, J.C; OLIVEIRA, M. Um olhar dos estudantes do curso de biblioteconomia acerca do que são dados, informações e conhecimentos. Informação & Informação. Londrina, v. 25, n. 2, p. 484 – 508, abr./jun. 2020.
Marciano, João Luiz Pereira. **Segurança da informação : uma abordagem social:** contribuição da Universidade de Brasília. 2016. Tese (Doutorado)-Programa de Pós-Graduação em Ciências da Informação do Departameto de Ciências da Informação. Disponível em: < https://repositorio.unb.br/handle/10482/1943>. Acesso em: 10, mar. 2022.

NAKAMURA, Emílio Tissato. **Segurança da informação e de redes.** Londrina: 2016. Disponível em: < https://docplayer.com.br/155995870-Seguranca-da-informacao-e-de-redes.html>. Acesso em: 22, fev. 2022

NETO, Pedro Tenório Mascarenhas; ARAÚJO, Wagner Junqueira. **Segurança da Informação:** Uma visão sistêmatica Para Implatação em organzações. Paraíba: 2019. Disponível em: <http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/download/209/75/905-1?inline=1>. Acesso em: 20, mar. 2022

NEVES, Felipe Campos at, al. **Implantação de *Firewall* Pfsense**. 2014, Monografia (Conclusão do curso)- Universidade Tecnológica Federal do Paraná. Departamento
Acadêmico de Eletrônica. Disponível em: < https://repositorio.utfpr.edu.br/jspui/bitstream/1/9787/2/CT_COTEL_2014_2_02.pdf>. Acesso em: 03, maio 2022.

O COMEÇO DO PFSENSE. **Electric Sheep Fencing**, 2022. Disponível em: < https://www.pfsense.org/getting-started/>. Acesso em 12, maio. 2022.

OROZCO, Alex Mulattieri Suarez. **Balanceamento entre segurança e desempenho na comunicação entre os planos de controle e dados em redes definidas por *Software***: contribuição da Pontifícia Universidade Católica do Rio Grane do Sul. 2018.Tese (Doutorado)- Pontifícia Universidade Católica do Rio Grane do Sul, Programa de Pós-Graduação em Ciência da Computação. Disponível em: < https://repositorio.pucrs.br/dspace/bitstream/10923/14903/1/000493958-Texto%2bCompleto-0.pdf>. Acesso em: 20, fev. 2022.

PAZ, Nathalia. O que é segurança da informação e como fortalecer na sua empresa. **Idblog**, 2021. Disponível em: < https://blog.idwall.co/o-que-e-seguranca-da-informacao/?utm_term=&utm_campaign=Google_Search_Perf-conv_Nacional_Blog_DSA&utm_source=adwords&utm_medium=ppc&hsa_acc=4544575733&hsa_cam=14824085929&hsa_grp=128729978878&hsa_ad=576349187712&hsa_src=g&hsa_tgt=dsa41848713900&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjwuMuRBhCJARIsAHXdnqOnIRDCC0u6SygeJKhLuehrD3zY29ChWgOthGipdOWGR_DqGnC5ljUaAjlNEALw_wcB> Acesso em: 03, mar. 2022.

PETTERS, Jeff. COMO USAR O WIRESHARK: TUTORIAL COMPLETO E DICAS.

Varonis, 2020. Disponível em: < https://www.varonis.com/pt-br/blog/how-to-use-wireshark> . Acesso em: 01, Ago. 2022.

PFSENSE: TUDO QUE VOCÊ PRECISA SABER. **Techlise**, 2020. Disponível em: < https://www.techlise.com.br/blog/pfsense-tudo-que-voce-precisa-saber/>. Acesso em: 25, abr. 2022.

RAIMUNDO,Bruno et, al. *Endian Firewall*. **Brasil** Documentos, 2011. Disponível em: < https://fdocumentos.tips/document/*Endian-Firewall*-5584ae0bd69d7.html>. Acesso em: 15, maio. 2022.

RED TEAM E BLUE TEAM. **Acadi-ti,** 2022. Disponível em: < https://acaditi.com.br/red-team-e-blue-team/> . Acesso em: 20, jun. 2022.

RED, PURPLE, AND BLUE: AS CORES DE UM PROGRAMA DE TESTES DE SEGURANÇA CIBERNÉTICA. **Minuto da Segurança,** 2022. Disponível em: < https://minutodaseguranca.blog.br/red-purple-and-blue-as-cores-de-um-programa-de-testes-de-seguranca-cibernetica/> . Acesso em: 25, jun. 2022.

REQUISITOS DE *HARDWARE FIREWALL ENDIAN*. **Cop e Direita,** 2022. Disponível em: < http://ptcomputador.com/Networking/network-security/76497.html>.
Acesso em: 10, abr. 2022.

SANTOS, Ronan Leandro Coelho. **Aspectos da Segurança da Informação.** Sua Importância para as Organizações, Minas Gerais, 2019. Disponível em: < https://ri.unipac.br/repositorio/wp-content/uploads/2019/08/Ronan.pdf> . Acesso em: 25, mar. 2022.

SEGURANÇA DA INFORMAÇÃO CONCEITOS E MECANISMOS. **Oficina da Net,** 2018. Disponível em: < https://www.oficinadanet.com.br/artigo/1307/seguranca_da_informacao_conceitos_e_mecanismos>. Acesso em: 12, mar. 2022.

ZEFERINO, Denis. O que é Segurança da Informação e qual sua importância?. **Certifique,** 2020. Disponível em:< https://www.certifiquei.com.br/seguranca-informacao/#:~:text=Seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o%2

0%C3%A9%20um,toda%20organiza%C3%A7%C3%A3o%20gera%20informa%C3%A7%C3%B5es%20pr%C3%B3prias.> Acesso em : 01, mar. 2022.

APÊNDICE A – KALI LINUX

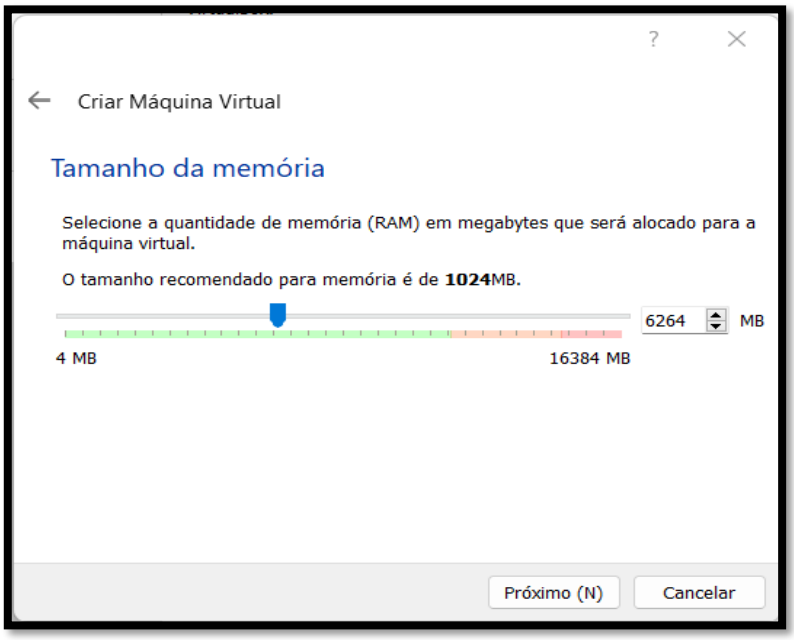
Este apêndice mostra todo o passo a passo da instalação do software Kali linux

.

A instalação do Kali Linux foi realizada da seguinte maneira:

Depois de executar o download da imagem ISO do Kali Linux, em seguida foi configurado um servidor Linux, para instalação do hacker. Foram alocados 3 processadores e 30GB de memoria para armazenamento no disco. Como pode ser visto na Figura 33, foram alocados também 6GB de memoria RAM, pois a maioria dos ataques e feito pela força bruta e tentativa e erro.

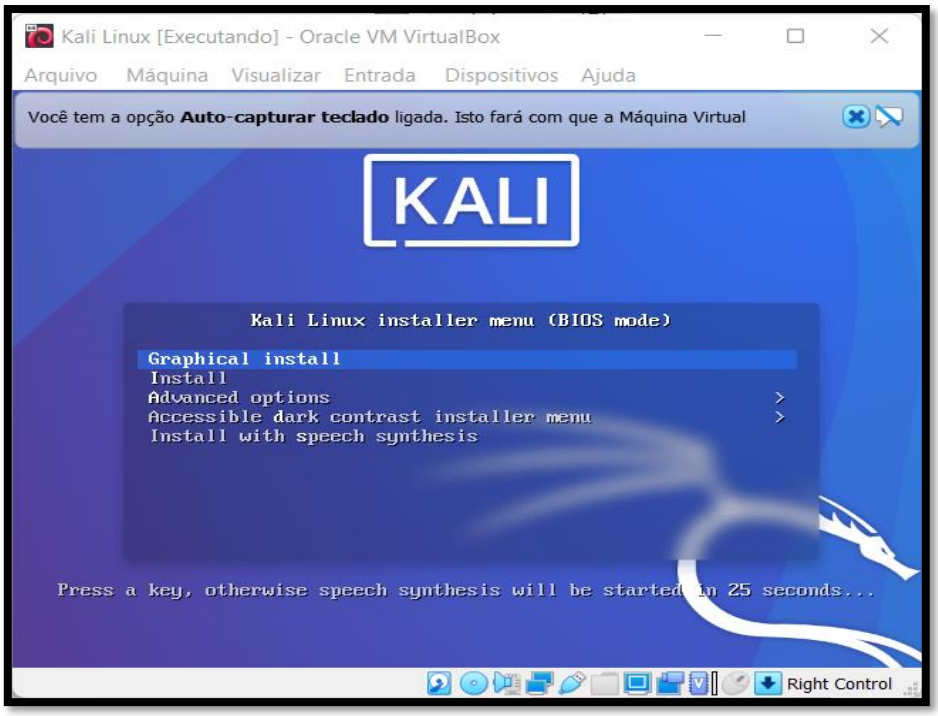
Figura 33 – Memoria RAM Alocada Kali



Fonte: Autoria Própria, 2022

A Figura 34 mostra que depois de iniciar o servidor, foi escolhida a primeira opção "*Graphical install*", ou instalação com interface gráfica. Em seguida, foi escolhido o idioma, localidade e configuração do teclado, ambos Português Brasil.

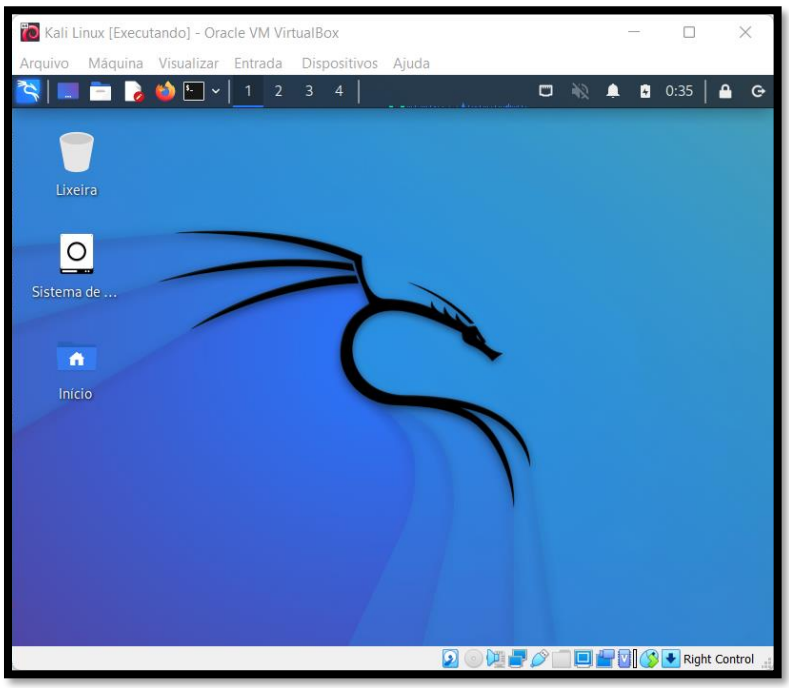
Figura 34 – Instalação Grafica



Fonte: Autoria Própria, 2022

Terminada a instalação do Kali Linux foram configurados um novo usuário e senha para acessar a maquina, o relógio que a maquina vai seguir, finalizando com a configuração da partição do disco. A Figura 35 mostra a tela inicial do Kali Linux.

Figura 35 – Tela Inicial Kali Linux



Fonte: Autoria Própria, 2022

Na tela incial do Kali linux pode-se observar onde fica o terminal , que sera a ferramenta utilizada para rodar os camandos de ataque .