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

SEGURANÇA DE REDES DE COMPUTADORES: UM ESTUDO SOBRE O ENDIAN FIREWALL

JOSÉ RODRIGO DA FONSECA GOMES

GOIÂNIA
2023

JOSÉ RODRIGO DA FONSECA GOMES

SEGURANÇA DE REDES DE COMPUTADORES: UM ESTUDO SOBRE O ENDIAN FIREWALL

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

Orientadora: Prof. Dra. Solange da Silva

Banca examinadora: Prof. Me. Wilmar Oliveira de Queiroz

Prof. Me. Rafael Leal Martins

GOIÂNIA

2023

JOSÉ RODRIGO DA FONSECA GOMES

FIREWALL ENDIAN PARA SEGURANÇA DE REDES DE COMPUTADORES DOMÉSTICA E CORPORATIVA

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 e de artes, da Pontifícia Universidade Católica de Goiás, em __/__ /__/

Banca Examinadora:

_____

Orientadora: Profa. Dra. Solange da Silva

_____

Prof. Me. Wilmar Oliveira de Queiroz

_____

Prof. Me. Rafael Leal Martins

GOIÂNIA

2023

AGRADECIMENTOS

Agradeço a Deus, por me dar forças para continuar persistindo ao longo do curso.

A minha mãe, Maria José da Fonseca, que sempre me apoiou, e me incentivou a estudar, única herança que poderia deixar pra mim.

A bolsa de estudos social, fornecida pela PUC GO, que foi de grande ajuda na minha saúde financeira, possibilitando estudar nesta instituição de grande respeito.

A minha prezada e querida orientadora, Profa. Dra. Solange da Silva, pelos seus ensinamentos, conhecimentos e compreensão durante toda nossa jornada.

A minha família e amigos que sempre me ajudaram ao longo do curso.

A todos, que de uma maneira ou de outra, colaboraram para o êxito deste trabalho.

RESUMO

O objetivo geral deste trabalho foi o de identificar e descrever as funcionalidades do *Firewall Endian*, usados em redes de computadores. Quanto ao aspecto metodológico está pesquisa é bibliográfica e experimental. O estudo permitiu concluir com os experimentos realizados, tais como a instalação do Kali Linux, a configuração do *Proxy* para bloquear sites específicos e a implementação do *OpenVPN*. Eles proporcionaram uma aplicação prática das funcionalidades do *Endian Firewall* e comprovando sua eficacia. A configuração do *firewall* para permitir o tráfego desejado e a criação de regras específicas, como o redirecionamento de portas para a área de trabalho remota, demonstrou a flexibilidade e adaptabilidade do sistema às necessidades do administrador de rede. Observou-se também que a instalação e configuração bem-sucedidas do Endian *Firewall*, aliadas aos experimentos realizados, destacaram a eficácia e a versatilidade desta ferramenta como uma solução de segurança robusta para ambientes de rede. A compreensão das diversas funcionalidades oferecidas pelo *Endian Firewall* possibilita seu uso em ambientes empresariais e residenciais, proporcionando controle e proteção eficazes contra ameaças de segurança.

Palavras chaves: Firewall, Endian Firewall, redes de computadores, segurança da informação

ABSTRACT

The general objective of this work was to identify and describe the functionalities of the Endian Firewall, used in computer networks. Regarding the methodological aspect, this research is bibliographic and experimental. The study allowed us to conclude with the experiments carried out, such as installing Kali Linux, configuring the Proxy to block specific websites and implementing OpenVPN. They provided a practical application of Endian Firewall's functionalities and proved its effectiveness. Configuring the firewall to allow the desired traffic and creating specific rules, such as port forwarding for remote desktop, demonstrated the system's flexibility and adaptability to the needs of the network administrator. It was also observed that the successful installation and configuration of Endian Firewall, combined with the experiments carried out, highlighted the effectiveness and versatility of this tool as a robust security solution for network environments. Understanding the various functionalities offered by Endian Firewall enables its use in business and residential environments, providing effective control and protection against security threats.

Keywords: Firewall, Endian Firewall, computer networks, information security

Lista de Figuras

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CPU	*Central Processing Unit* ou Unidade Central de Processamento
DNS	*Domain Name System* ou Sistema de Nome de Domínio
EFW	*Endian Firewall Community*
GHz	*Gigahertz*
GB	*Gigabyte*
Gw2Gw	*Gateway-to-Gateway*
HTTP	*Hypertext Transfer Protocol* ou Protocolo de Transferência de Hipertexto
HD	*Hard Disk* ou Disco Duro
IPS	In-Plane Switching ou Comutação no plano
IDS	*Intrusion Detection System* ou Sistema de Detecção de Intrusos
IEC	*International Electrotechnical Commission* ou Comissão Eletrotécnica Internacional
ISO	*International Organization for Standardization* ou Organização Internacional de Normalização
MB	*MegaByte*
NIC	O Núcleo de Informação e Coordenação
NAT	*Network Address Translation* ou Tradução do Endereço da Rede
QoS	*Quality of Service* ou Qualidade de Serviço
SGSI	Sistema de Gestão de Segurança da Informação

SSD	*Solid State Drive* ou Unidade de Estado Solido
SMB	Server Message Block ou Bloco de Mensagem de Servidor
RAM	*Random Access Memory* ou Memoria de Acesso Aleatóri
SI	Segurança da Informação
SSL	*Secure Sockets Layer* ou Camada de Soquetes Seguro
PSK	*Pre-Shared Key* ou *PSK*
TCC	Trabalho de Conclusão de Curso
UTM	*Unified Threat Management* ou Gerenciamento Unificado de Ameaças
VPN	*Virtual Private Network* ou Rede Privada Virtual
VM	*Virtual Machine* ou Maquina Virtua

SUMÁRIO

1 INTRODUÇÃO

Redes de computadores é um conjunto de computadores conectados por uma tecnologia. Mais de dois computadores conectados e trocando informação podem ser considerada uma rede. Essa conexão pode ser com fio ou sem fio, podendo ser por rede óptica, ondas de infravermelho, redes de satélites. Existem redes de diversas formas e modelos, operando com suas próprias regras. Essas redes conectadas a outras redes formam redes maiores e o nosso melhor exemplo é a própria Internet (Molina, Silveira & Santos, 2019).

Conforme Morais (2021), Segurança da Informação (SI) é um conjunto de dados, estruturado e organizado, dando um contexto aos dados e produzindo conhecimento. Esse conhecimento vem a ser útil a outra pessoa ou organização, podendo empregar uso criminoso a esses dados, prejudicando o dono original.

Um *firewall* é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos, de acordo com um conjunto definido de regras de segurança, a ser definidas pelo administrador (CISCO, 2023).

A questão de segurança em redes de computadores, tanto em redes domésticas quando corporativas, vem se tornando algo muito importante desde o surgimento da rede em si. Como na Internet, por exemplo, desde ataques para capturar senhas, dados, capturar tráfego de dados e encontrar vulnerabilidades no geral (Molina, 2018).

Desde o surgimento da Internet o ser humano se torna dependente da tecnologia. No decorrer dos anos essa dependência fica mais evidente, uma vez que existem sistemas bancários e gerenciamento de empresas na Internet. Uma ferramenta essencial na sociedade (Sousa, 2010).

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 (Dourado, 2022).

O *Endian Firewall Community* (EFW) é um produto de segurança pronto para uso, baseado em Linux, projetado para uso doméstico ou empresarial, que pode transformar

qualquer dispositivo de hardware não utilizado em uma solução de Gerenciamento Unificado de Ameaças (UTM) com todos os recursos (ENDIAN, 2023).

Justifica estudar esse tema pois, o uso do firewall é importante para proteção em redes de computadores. Esses firewalls atuam como a primeira linha de defesa. Uma das várias 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).

Diante deste contexto, esse trabalho visa responder a seguinte questão de pesquisa: - **Quais as funcionalidades do software de segurança Endian *Firewall Community*?**

Este trabalho tem o objetivo geral de identificar e descrever as funcionalidades do software de segurança Endian *Firewall Community*.

Os objetivos específicos são:

- descrever o funcionamento do software de segurança Endian *Firewall*
- Mostrar o passo a passo da instalação do Endian *Firewall*
- implementar as funções: *OpenVPN, Proxy* e *Firewall* para verificar a eficácia deste *firewall*;

Espera-se que os resultados deste trabalho possam contribuir:

• Informando aos administradores de redes corporativas sobre alguns softwares que podem garantir a segurança da informação;

• 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 e apresentando as normas de segurança existentes.

Quantos aos aspectos metodológicos, esta pesquisa em relação aos procedimentos técnicos, é uma pesquisa bibliográfica.

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 de pesquisa, objetivos e resultados esperados. O Capítulo 2 traz 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 o software Endian *Firewall*, mostrando suas funcionalidades. O Capítulo 5 traz as funções de *OpenVpn, Proxy e Firewall* do *Endian*, especificando suas ferramentas. O capitulo 6 mostra as funções citadas, assim como suas configurações, testando/demostrando parte delas. O capitulo 7 traz as considerações finais.

2 REFERENCIAL TEÓRICO

Este capítulo é composto de duas partes: a primeira apresentando conceitos e definições da área e a segunda trazem alguns trabalhos relacionados ao tema.

2.1 Segurança da informação

A SI é a proteção de dados de propriedade de organizações ou pessoas de ameaças diversas. É um esforço em constante desenvolvimento, com ações que visão bloquear esses ataques e garantir a segurança dos dados (FIA, 2022).

A segurança da informação SI está intrinsecamente ligada à salvaguarda de um conjunto de dados, visando preservar o valor que essas informações têm para um indivíduo ou uma organização. As propriedades fundamentais da segurança da informação incluem confidencialidade, integridade, disponibilidade, autenticidade e legalidade (Wikipedia, 2019).

A tríade CIA (Confidencialidade, Integridade e Disponibilidade) orienta a segurança da informação, sendo complementada por atributos como não-repúdio, autenticidade e conformidade. Com o avanço do comércio eletrônico e da sociedade da informação, a privacidade também é uma preocupação crucial.

Os atributos básicos da segurança da informação, segundo padrões internacionais (ISO/IEC 17799:2005), são:

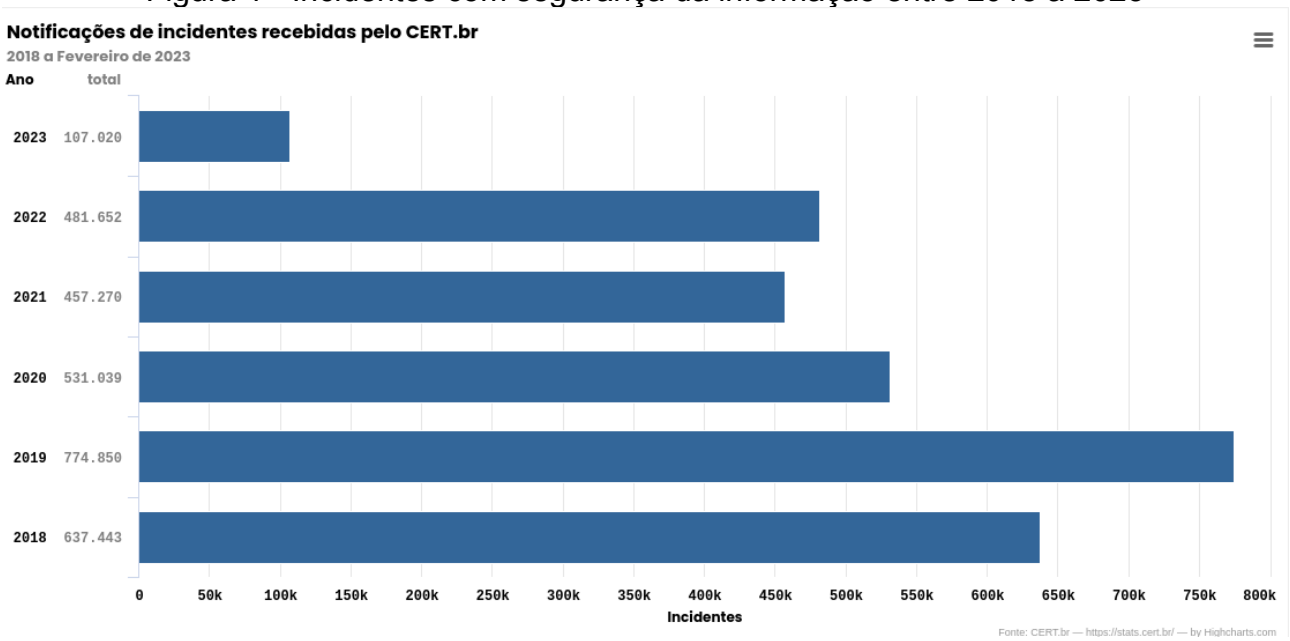
- Confidencialidade: Limita o acesso à informação a entidades autorizadas.
- Integridade: Garante que a informação mantenha suas características originais, incluindo controle de mudanças e ciclo de vida.
- Disponibilidade: Assegura que a informação esteja sempre disponível para uso legítimo.
- Autenticidade: Certifica que a informação provém da fonte anunciada e não foi alterada durante o processo (Wikipedia, 2019).

O Centro de Estudos, Respostas e Tratamentos (CERT.br) é um grupo de respostas às incidências de insegurança de dados do Brasil, de Responsabilidade

Nacional de último recurso, mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br). O NIC.br é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no Brasil.

A Figura 1 apresenta as incidências recebidas pelo CERT.br, de 2018 a 2023. Observa-se que a cada ano aumenta o número de ataques.

Figura 1 - Incidentes com segurança da informação entre 2018 a 2023



Fonte: cert.br, 2023

2.2 Firewall

Um *firewall* é um dispositivo de segurança de rede que controla o tráfego, decidindo permitir ou bloquear com base em regras definidas. Essa tecnologia é a linha de defesa primária há mais de 25 anos, estabelecendo uma barreira entre redes internas protegidas e redes externas, como a Internet. *Firewalls* podem ser implementados como hardware, software ou ambos (Cisco Systems Inc. , 2023).

Existem dois tipos de *firewalls*: os *stateless* e os *stateful* e representam abordagens distintas para a filtragem de pacotes em uma rede. A diferença fundamental entre eles está na forma como lidam com a informação sobre as conexões. O *firewall Stateless*, ou sem estado, trata cada pacote de maneira independente, sem manter um conhecimento prévio das conexões. Isso significa que ele avalia cada pacote isoladamente, sem considerar o contexto da conexão. Por outro lado, o *firewall Stateful* ou com estado, utiliza uma tabela de estados ou conexões para manter um registro atualizado do estado de cada conexão que passa pelo dispositivo (OSTEC, 2020).

A abordagem *Stateful* oferece vantagens significativas, como a capacidade de produzir economias no número de regras, maior velocidade na validação das regras e, principalmente, maior segurança. Isso ocorre porque, ao manter informações sobre o estado da conexão, o *firewall* pode avaliar dados adicionais, além de endereços e portas, dependendo do protocolo de transporte utilizado. Embora o *Stateful* seja considerado uma evolução natural do *Stateless*, ambos continuam em uso e desempenham papéis essenciais em soluções de segurança da informação (OSTEC, 2020).

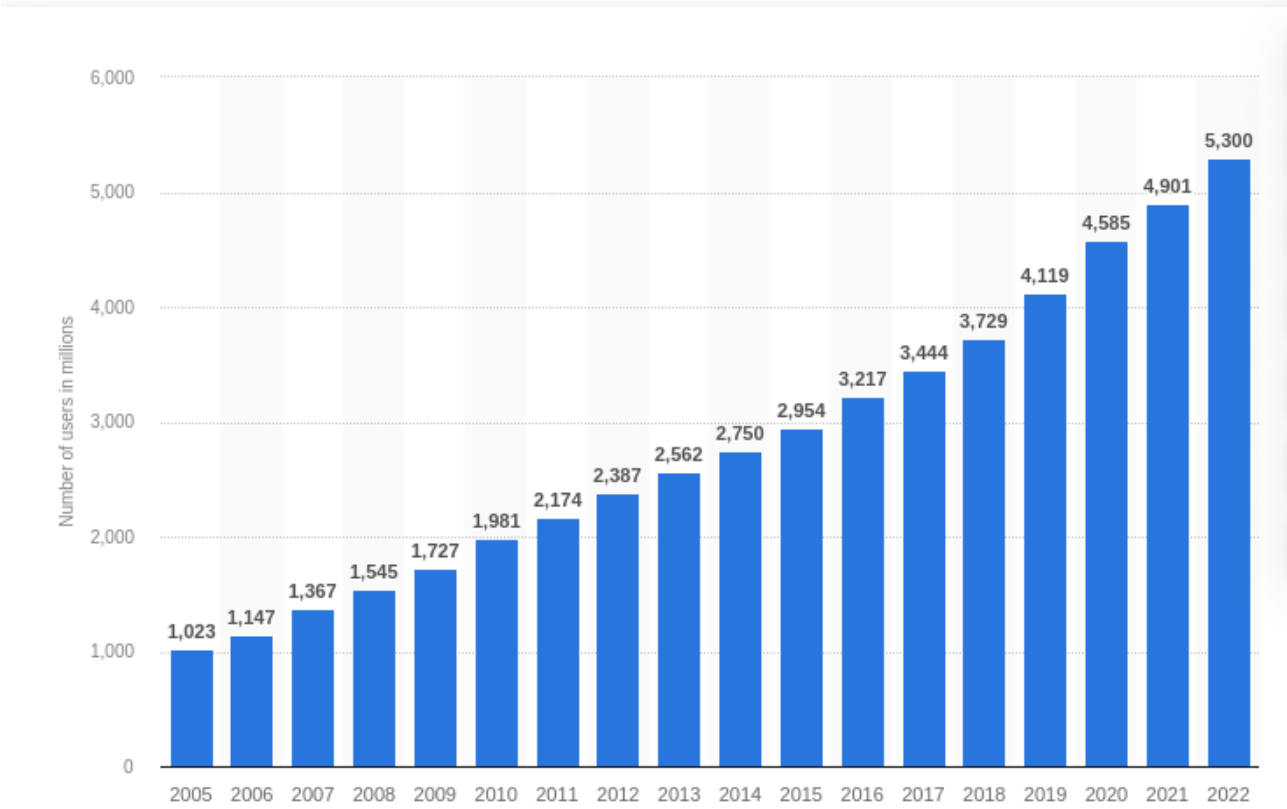
2.3 Redes De Computadores

Uma rede doméstica segura é um aspecto essencial da segurança na Internet. Os *hackers* podem explorar redes vulneráveis para realizar vários tipos de ataques, como instalar *malware*, roubar dados e identidade e criar *botnets* (KASPERSKEY, 2023).

Em 2021, o número de domicílios com acesso à internet no Brasil chegou a 90,0%, segundo dados da Pesquisa Nacional por Amostra de Domicílios. São 65,6 milhões de domicílios conectados, 5,8 milhões a mais do que em 2019 (GOV, 2022).

Na Figura 2 pode-se perceber um número crescente de usuários de redes de computadores, totalizando 5.300 milhões em 2022, no Brasil e no Mundo (CERT.br, 2023).

Figura 2 - Estimativa de pessoas com acesso a internet no mundo.



Fonte: cert.br, 2023

De acordo com gráfico percebe-se uma quantidade absurda de pessoas com acesso a rede.

2.3.1 ISO/IEC 27000

ISO é a sigla para *International Organization for Standardization*. Objetivo desenvolver e promover normas, testes, padronizações e certificações que facilitam as relações entre diferentes nações. ISO foi fundada em 1947 e hoje conta com membros de 165 países. No Brasil, ela é representada pela Associação Brasileira de Normas Técnicas (ABNT).

ISO 27000 é um conjunto de certificações de segurança da informação e proteção de dados para empresas e órgãos públicos. Elas servem como base para a criação de um

Sistema de Gestão de Segurança da Informação (SGSI) em organizações de pequeno, médio e grande porte (PUCPR, 2021).

A primeira versão é de 2005, padrão britânico de segurança da informação. Hoje está em vigor a ISO/IEC 27000:2018. Ela traz alguns princípios norteadores da segurança da informação. Os principais são: confidencialidade, integridade, disponibilidade e autenticidade (PUCPR, 2021).

2.3.2 ISO/IEC 27001

Esta Norma ISSO/IEC 27001 traz os requisitos necessários para a implantação de um SGSI. Eles podem ser resumidos em 5 fases. Entender o contexto da organização: ela já tem um SGSI? Como ela lida com a segurança da informação? Avaliação de riscos: além de identificar riscos e oportunidades, é preciso conscientizar toda a empresa sobre a importância da segurança da informação.

Controles operacionais: o objetivo é controlar, eliminar e diminuir a classificação dos riscos levantados na etapa anterior. Análise de eficácia: é feita uma auditoria interna para verificar o resultado da implantação dos controles operacionais. Melhoria: processo contínuo após o estabelecimento da certificação. A avaliação e controle de riscos devem ser feitos com frequência (PUCPR, 2021).

2.3.3 ISO/IEC 27002

Segundo Rodrigues (2021), a ISO 27002 funciona como um código de prática para controles de segurança. Ela descreve as melhores práticas para aqueles que implementam. Fornecendo diretrizes sobre a seleção, implementação e gerenciamento de controles levando em consideração os ambientes de risco da organização. Pode ser usada por organizações que planejam implementar as suas próprias diretrizes de gerenciamento de segurança da informação. Utilizar a ISO 27002 traz vantagens significativas para a empresa como:

- Melhor consciência da segurança da informação;
- Maior controle de ativos e informações confidenciais;
- Fornece uma abordagem para implementação de políticas de controle;
- Oportunidade de identificar e corrigir deficiências;
- Reduzir o risco de responsabilidade por não implementar um SGSI ou determinar políticas e procedimentos;
- Torna-se um diferencial competitivo para a conquista de clientes que valorizam as melhores práticas do mercado;
- Melhor organização com processos e mecanismos bem projetados e gerenciados;
- Promove redução de custos com prevenção de incidentes de segurança da informação;
- Conformidade com a legislação e outros regulamentos.

2.3.4 ISO/IEC 27003

A Norma ISO/IEC 27003 sugere orientações necessárias para aplicação do SGSI na empresa, desde a concepção do projeto até a elaboração dos planos para implantá-lo no campo prático.

Basicamente, a ISO/IEC 27003 informa o procedimento a ser realizado para que o SGSI seja bem-sucedido, que engloba etapas tais como:

- Obtenção da aprovação da alta administração para iniciar o projeto;
- Definição do escopo, políticas e limites;
- Estudo dos requisitos de segurança da informação;
- Condução da avaliação de riscos, bem como a forma que eles serão tratados;
- Definição do SGSI (IRKO, 2021).

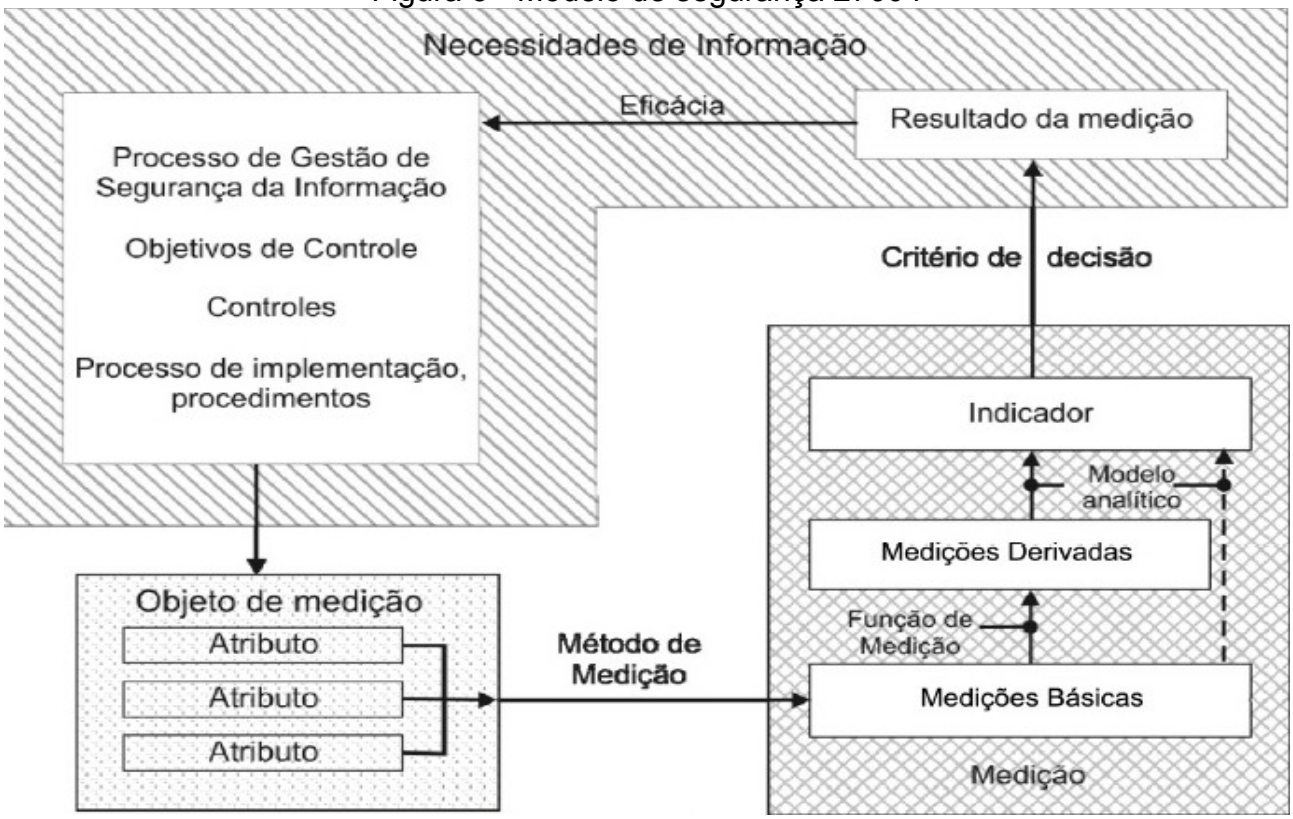
2.3.5 ISO/IEC 27004

A ISO/IEC 27004 define as métricas para gestão de segurança da informação, ou seja, como saber o nível de eficácia das medidas aplicadas. Seu conteúdo é separado em diferentes seções:

- Justificativa: explica a importância da medição;
- Características: explica o que deve ser medido, quem deve fazê-lo e quando;
- Tipos de medidas: lista medidas de desempenho eficientes e eficazes;
- Processos: mostra como desenvolver, implementar e aplicar métricas;
- Anexos: são 3 anexos que trazem modelos de medição, exemplos de métricas e fórmulas matemáticas.

Na Figura 3 visualiza-se um quadro desse modelo, onde é fornecido mais detalhes sobre o processo.

Figura 3 - Modelo de segurança 27004



Fonte: Qualidadeonline's Blog, 2023

2.4 Trabalhos relacionados

O estudo de Dourado (2022), foi focado em identificar e descrever as funcionalidades dos *firewalls Pfsense* e *Endian*, usados em redes de computadores. Entretanto, este estudo focou mais no *Endian Firewall*, por este ser menos explorado na literatura. 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 possível demonstrar que o *Endian Firewall* possui funcionalidades que realmente funcionam para bloquear os ataques ou acessos não permitidos.

O trabalho de Morais (2021), apresentar as normas ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27005, para mostrar um ataque de *ransomware*, como exemplo, sugerindo como um usuário pode se prevenir para garantir a segurança dos dados de seu computador. Os resultados mostraram como atacar um computador, usando o sistema operacional Kali Linux, por meio da ferramenta *The Fat Rat*, listando um passo a passo para criar um *ransomware*, como exemplo de como atacar um computador pessoal. O estudo permitiu concluir que as normas de políticas de segurança ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27005 tem como por princípios básicos a integridade, confidencialidade, disponibilidade de cada informação. Se as diretrizes destas normas forem aplicadas nas empresas, podem tornar as redes mais seguras contra os ataques cibernéticos, como por exemplo na prevenção de *malwares*, apresentado neste trabalho.

O trabalho de Brandão (2021), identifica problemas e riscos existentes nas redes sociais mais utilizadas, simulando um ataque envolvendo a técnica de enviar e-mails utilizando táticas da engenharia social para enganar e sequestrar dados de utilizadores de redes sociais. O estudo realizado permitiu identificar problemas rotineiros. Além de vários riscos em acesso a redes sociais. Os usuários precisam ser conscientizados e capacitados, visando ficarem mais observadores e saberem como agir ao receber os cenários dos atacantes nas redes sociais.

Machado (2021) identifica e descreve algumas formas de ataques aos dados mais conhecidas, apresentando os pontos de vulnerabilidade do acesso. Os resultados identificaram os seguintes ataques: *Port Scanning Attack*, *Phishing*, *Spoofing*, *Sniffinge*

SQL Injection. Ela concluiu que não existe uma única solução para evitar os ataques e resolver todos os problemas de vulnerabilidades da empresa. Entretanto, existem diversas formas eficientes de proteção e boas práticas, tais como o treinamento dos funcionários e manter políticas de segurança difundidas na organização.

Em (Conceição, 2018), o trabalho utiliza-se de um sistema *firewall* para ser o sistema de controle responsável por gerenciar o fluxo de dados. Utilizou-se uma abordagem sistêmica da área, com aspectos teóricos e práticos. Na parte teórica, discutiram-se os componentes necessários para o desenvolvimento do sistema *firewall*. Na parte prática apresentou-se os resultados através do desenvolvimento de um protótipo do sistema *firewall*. Utilizou-se simulações das aplicações das regras para ilustrar a utilidade do sistema *firewall* , conclui-se que, desenvolvendo um *firewall* com um protocolo *OpenFlow* é capaz de fornecer uma proteção com a mesma capacidade ou superior que os softwares disponíveis na época do estudo, outra conclusão foi falta de materiais sobre referencias metodológicos disponíveis na rede sobre o tema.

3 MÉTODO

> Segundo a natureza, esta pesquisa é um resumo de assunto, buscando explicar a área do conhecimento do projeto, mostrando sua evolução, linha cronológica, como resultado da investigação das informações obtidas, levando ao entendimento de suas causas e explicações de forma coerente (Wazlawick, 2014).

Segundo os objetivos, esta pesquisa é exploratória, pois tem como função preencher as lacunas que costumam aparecer em um estudo. Também é descritiva, porque visa expor as características, sem aprofundar no motivo delas.

Quanto aos procedimentos técnicos é uma pesquisa bibliográfica e experimental. Pesquisa bibliográfica implica o estudo de artigos, teses, livros e outras publicações usualmente disponibilizadas por editoras e indexadas, (Gil, 2017).

a) A escolha de um tema: **Quais as funcionalidades do software de segurança Endian *Firewall Community*?**

b) Levantamento bibliográfico preliminar para realizar uma bibliográfica para auxiliar na definição do problema – Foram realizadas buscas no Periódicos da Capes e buscas no Google.

c) Busca das fontes: a pesquisa foi realizada em artigos, TCCs, sites, blogs,nas bases dos periódicos da CAPES e livros.

d) Fichamento: foi realizado resumo do material lido.

e) Redação do texto: escrita do TCC1.

A pesquisa experimental consiste em estabelecer um objeto de estudo, escolher as variáveis que a influenciam e determinar as formas de controle 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).

A pesquisa experimental é composta das seguintes etapas, conforme Gil (2017):

a) Formulação do problema: **Quais as funcionalidades do software de segurança Endian *Firewall Community*?**

b) Definição do plano experimental: descrever a configuração das ferramentas do Endian tais como: *OpenVPN, Proxy e Firewall.* Criar um túnel VPN e configuração de “cliente”, software que realiza a conexão com o servidor, configuração de bloqueio de

sites, usando ferramentas do Endian, localizadas na aba *proxy* e configuração de regra de entrada e saída, para permitir a conexão vinda de fora e saída.

c) Determinação do ambiente: foi usado o *Virtual Box* para simular dois ambientes (Maquina Kali e o servidor Endian). Servidor do Endian com 20GB de espaço em disco, 1024 de RAM, com um processador com 2 núcleos, versão community-x64_3.3.2. Uma maquina com o Kali, 2048MB de RAM, processador de 2 núcleos, armazenamento dinâmico (se expande, se necessário), versão 2022.3

d) Coleta de dados: testes realizados em maquinas virtuais, descritas no passo anterior, com base em configuração de *OpenVPN, Proxy e Firewall*, nos quais pelo menos uma configuração foi realizada em cada um destes.

e) Análise e interpretação dos dados: foram analisados os resultados obtidos de acordo com os testes realizados na coleta de dados.

f) Redação do relatório: foi registrada a pesquisa na escrita do TCC.

4 DESCRIÇÃO DE FUNCIONALIDADES DO *ENDIAN FIREWALL*

Este capítulo traz a descrição e o funcionamento do *Firewall* no *software Endian*.

4.1 Visão geral do *Endian firewall*

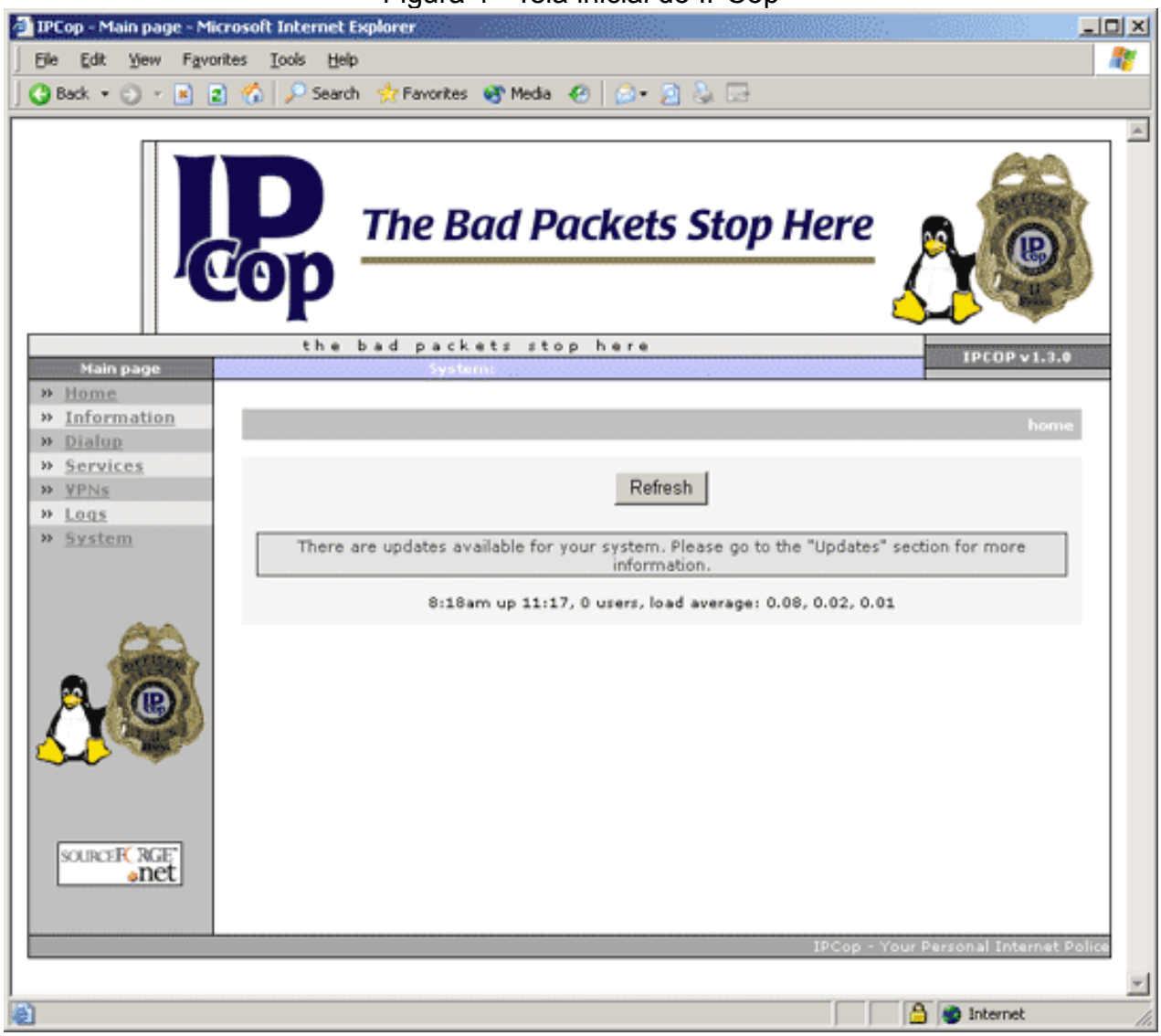
O *Endian* se enquadra na classe *Stateful Firewall*. Isso significa que o sistema não se limita a configurações e regras, mas, também, realiza rastreamento e monitoramento das conexões de rede e respectivos pacotes. Além disso, o software pode funcionar como antivírus, uma solução completa para controlar e manter uma rede contra ataques cibernéticos, como por exemplo *Ransomware*, ataque que vem fazendo vitimas recentes no Brasil (Delfino, 2023).

O Endian *Firewall* é uma distribuição Linux especializada em roteamento/*firewall* que possui uma interface unificada de gerenciamento. Foi originalmente baseado no *IPCop*, sendo que este é um *fork* do projeto *Smoothwall*, ele é um poderoso sistema de segurança, de código aberto, baseado em Linux e mantido por sua comunidade (Fonseca, 2014).

O IPCop é *Firewall* que possui um *kernel* próprio e diversas ferramentas integradas, como VPN, IDS, Proxy, Firewall, QoS e outras. Sua administração realizada via página WEB, com conexão SSL segura e criptografada, o que torna a ferramenta ainda mais interessante do ponto de vista de segurança (Cota, 2005).

A Figura 4 apresenta a tela inicial do *IPCop*, com as configurações básicas.

Figura 4 - Tela inicial do IPCop



Fonte: TechRepublic, 2023

4.2 Requisitos de Instalação

Os requisitos para a instalação do Endian podem variar de acordo com especificação da rede onde ele será instalado.

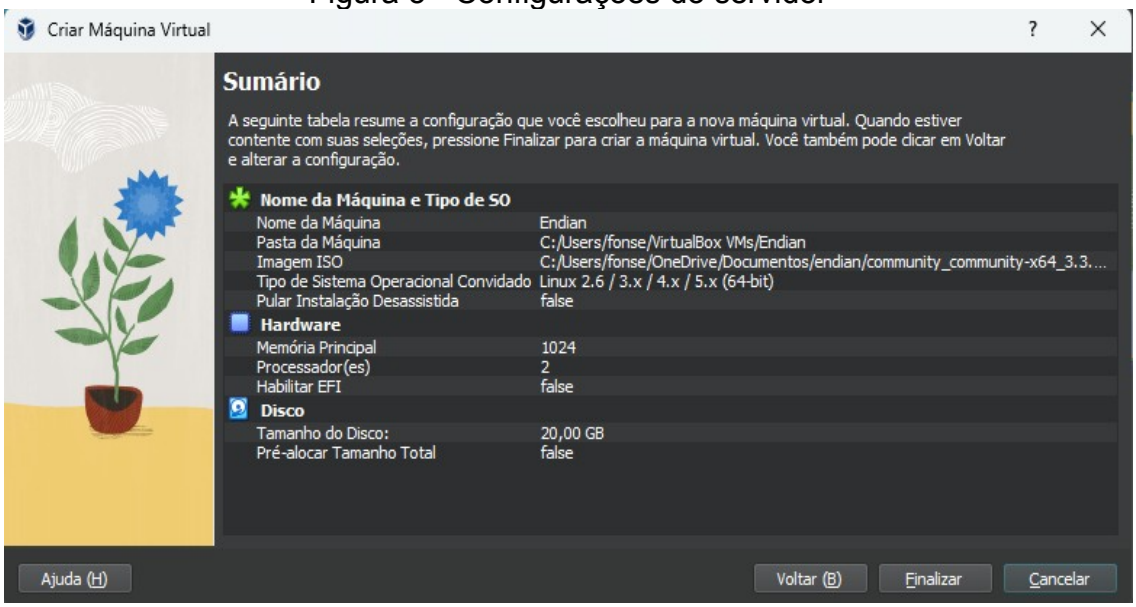
- CPU - Redes com até 25 usuários e 5 conexões VPN precisa de um processador de 1 GHz Pentium III. Rede com 50 usuários exigem um Pentium 4 rodando a 2.8 GHz ou mais rápido.
- RAM - Para redes menores, Será apenas 512 MB de RAM. Para maiores, Requer pelo menos 1 GB espaço no disco rígido.
- HD/SSD - Pequenas redes precisa de pelo menos 8 GB de espaço disponível no disco rígido, Maiores precisam de 20 GB de disco. Além desses pontos citados anteriormente, recomenda-se uma sistema de resfriamento extra, o sistema não comtava com pausas ou desligamento (PTCOMPUTADOR, 2023).

4.2.1 INSTALAÇÃO *ENDIAN FIREWALL*

A instalação do *Endian Firewall* foi realizada em uma máquina virtual.

Primeiro faz o *download* da Imagem do *software* no site oficial. Em seguida configura-se o ambiente, um servidor Linux, no qual foi instalado o *software. A* Figura 5 mostra as configurações do servidor, no qual foi alocado 20GB de espaço, 1024 de RAM, com um processador com 2 núcleos.

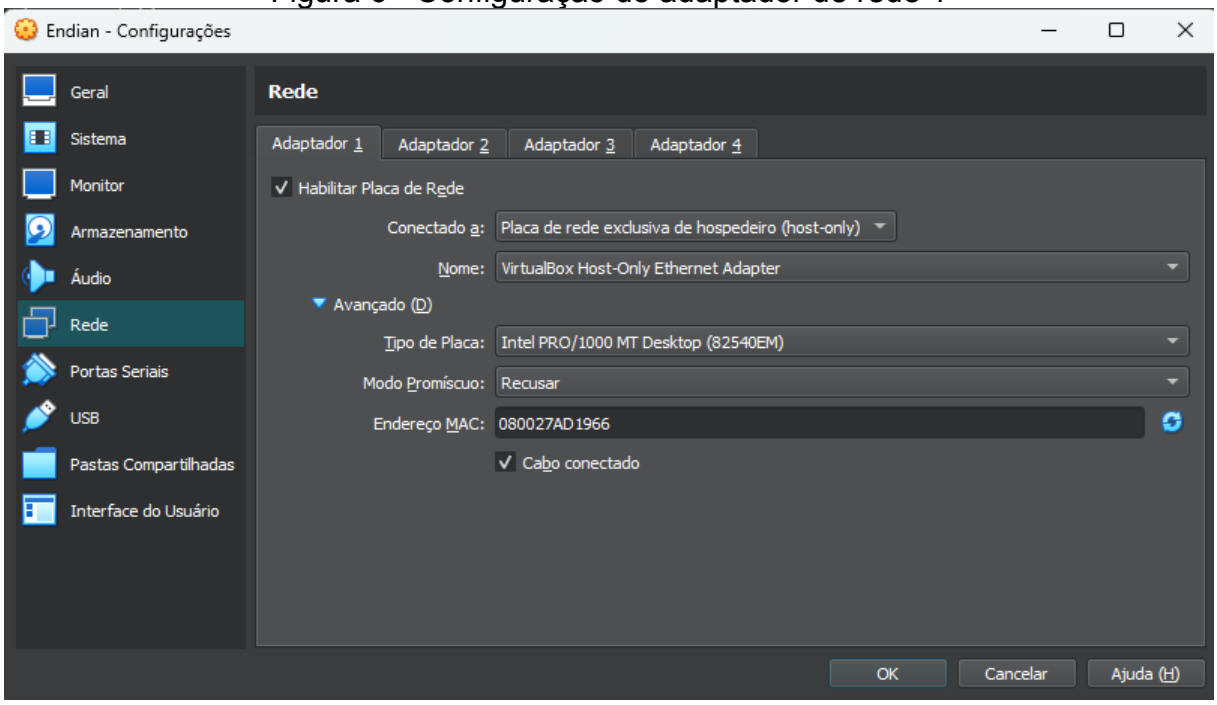
Figura 5 - Configurações do servidor



Fonte: autoria própria, 2023

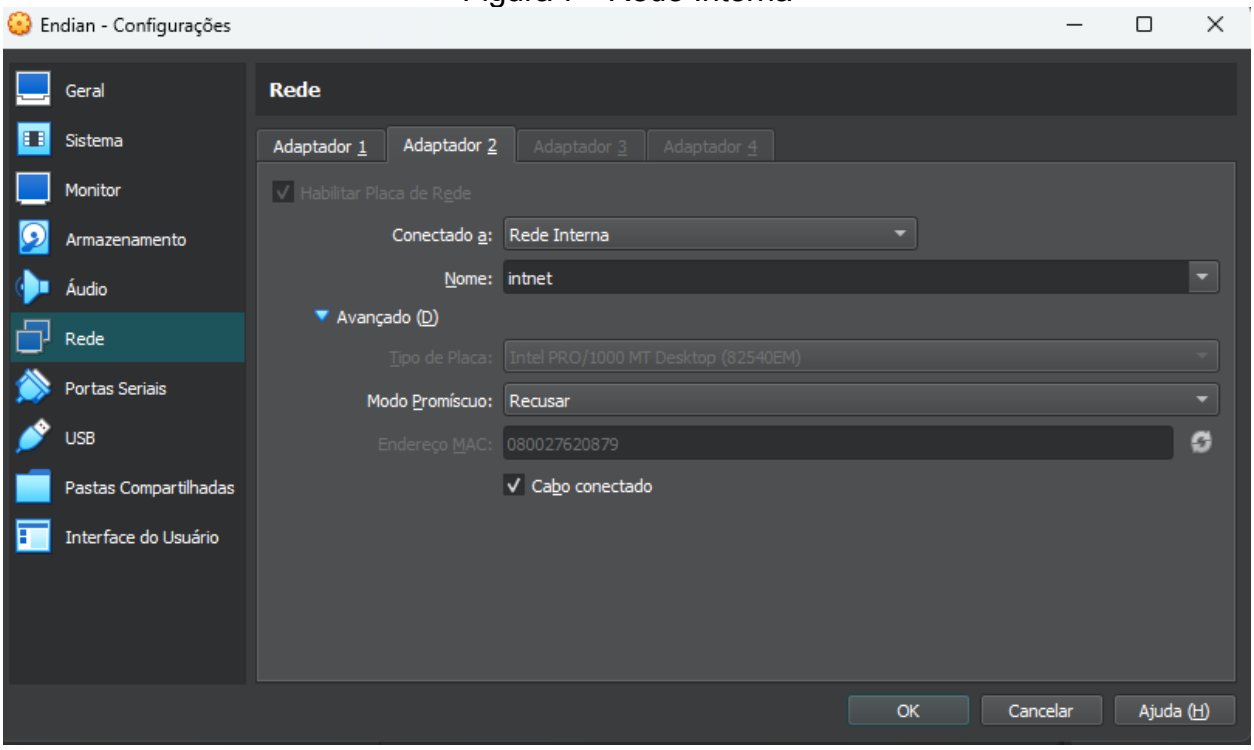
Foram configuradas duas portas para conexão de rede, a verde e a vermelho, portas essas que vão realizar a entrada e saída tráfego de dados, ilustradas nas Figuras 6 e 7. A Figura 6 apresenta uma configuração modo *HostOnly,* que funciona igual a Rede interna, porém com a vantagem de permitir que o *host* e outros computadores na mesma rede se conectem. A Figura 7 apresenta uma configuração modo Rede Interna, as VMs (Virtual Machine) conseguem ‘conversar’ entre si, mas não são visíveis pela rede do *Host*. Todos os pacotes ficam ‘escondidos’ na rede interna criada pelo *VirtualBox* , ou seja, o *Endian Firewall* funcionara internamente, sem acesso a rede externa (WL Tech, 2023).

Figura 6 - Configuração do adaptador de rede 1



Fonte: autoria própria, 2023

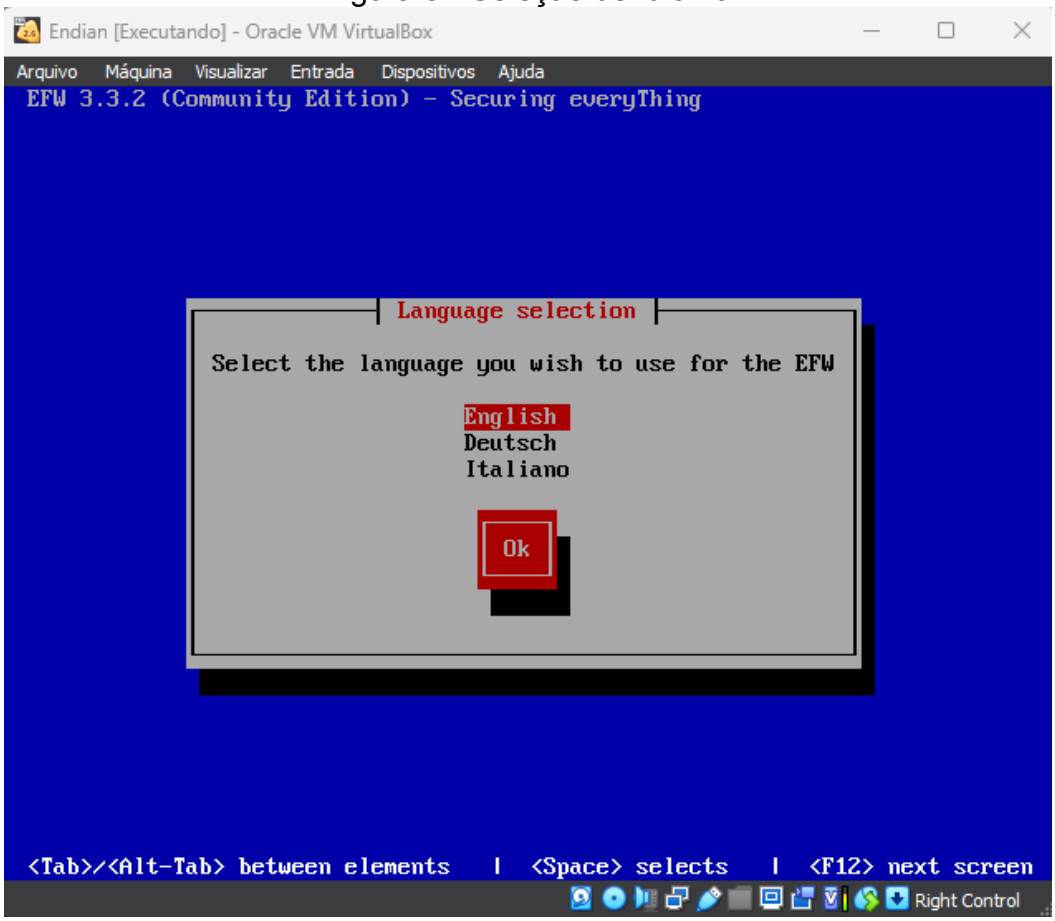
Figura 7 - Rede Interna



Fonte: autoria própria, 2023

Com a máquina configurada, é dado início ao processo de instalação do *Endian Firewall*. A Figura 8 mostra a primeira tela apresentada após o *boot* do sistema, que faz a seleção de idioma.

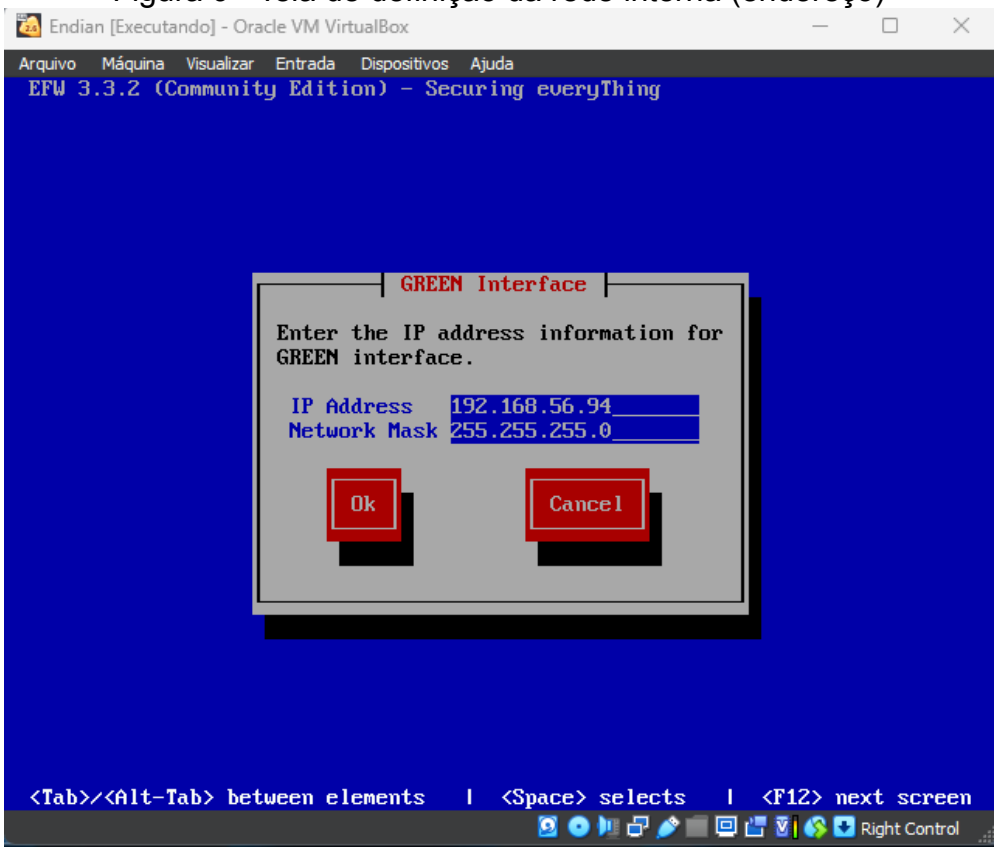
Figura 8 - Seleção de idioma



Fonte: autoria própria, 2023

Após a seleção do idioma, e realizada a instalação dos arquivos. Em seguida é apresentada a tela de configuração da rede verde, responsável pela rede interna, ilustrado na Figura 9.

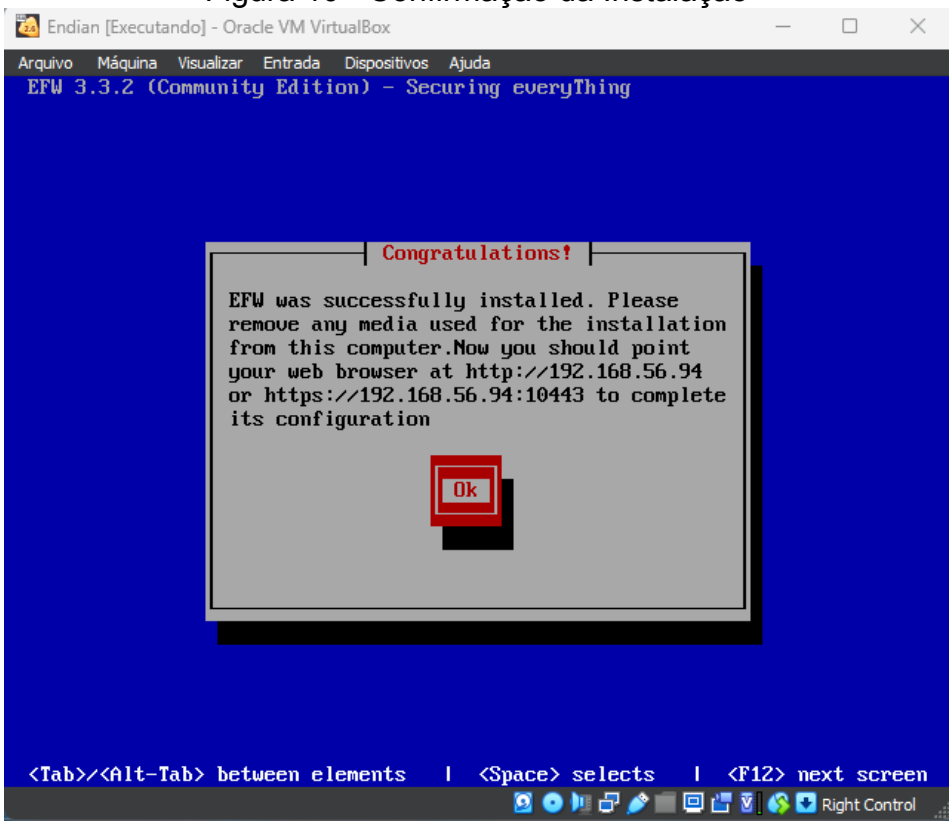
Figura 9 - Tela de definição da rede interna (endereço)



Fonte: autoria própria, 2023

Ao concluir a instalação do Endian *Firewall*, é apresentada uma mensagem de confirmação, apresentada na Figura 10, mostrando o endereço IP da *interface* WEB, composto pelo endereço definido na instalação seguido da porta de acesso. Nessa configuração podem ser definidas as configurações de *login*, tanto do portal, como servidor.

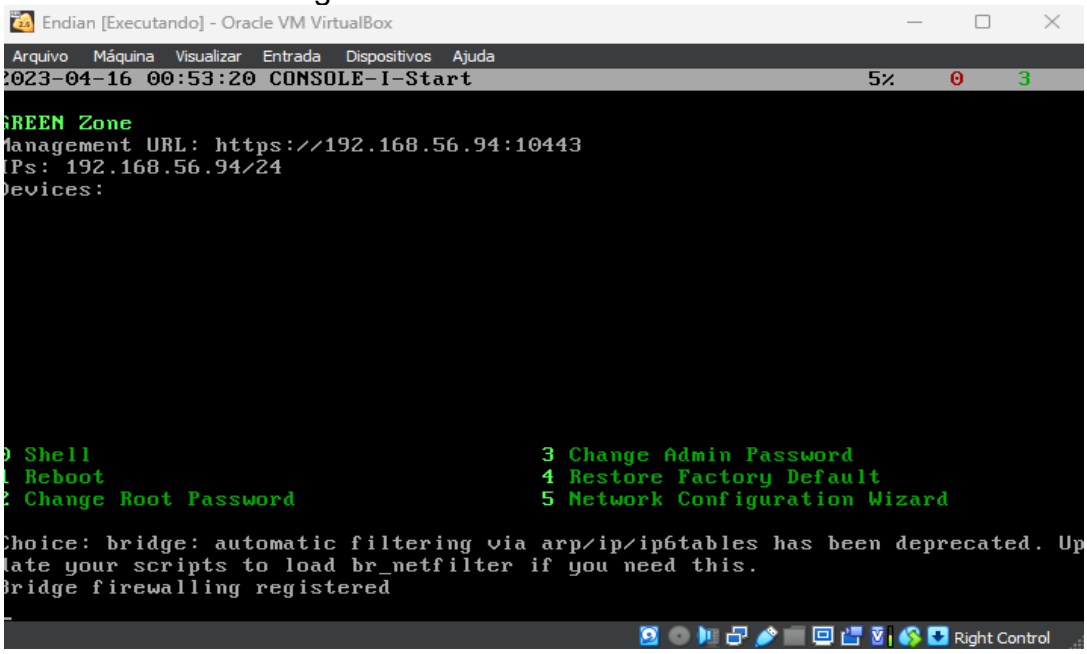
Figura 10 - Confirmação da Instalação



Fonte: autoria própria, 2023

A Figura 11 mostra a tela do servidor em si, após a instalação, na qual pode-se realizar algumas configurações. Neste trabalho de TCC, será tratado apenas a configuração WEB.

Figura 11 - Interface Endian Firewall

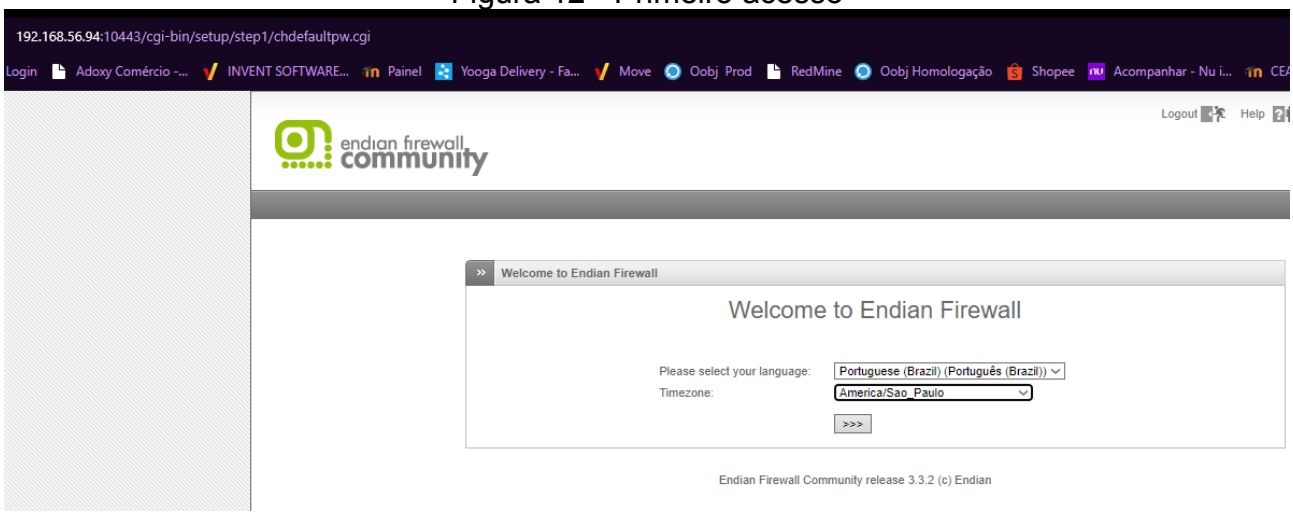


Fonte: autoria própria, 2023

4.2.2 PORTAL WEB

No portal WEB, acessado de uma terceira máquina, nesse caso, usado o navegador da máquina que está hospedando a VM do servidor Endian *Software*. Ao fazer o primeiro acesso aparece uma tela de agradecimentos, em seguida pede para definir o idioma do portal e a zona de fuso horário, conforme apresentado na Figura 12.

Figura 12 - Primeiro acesso

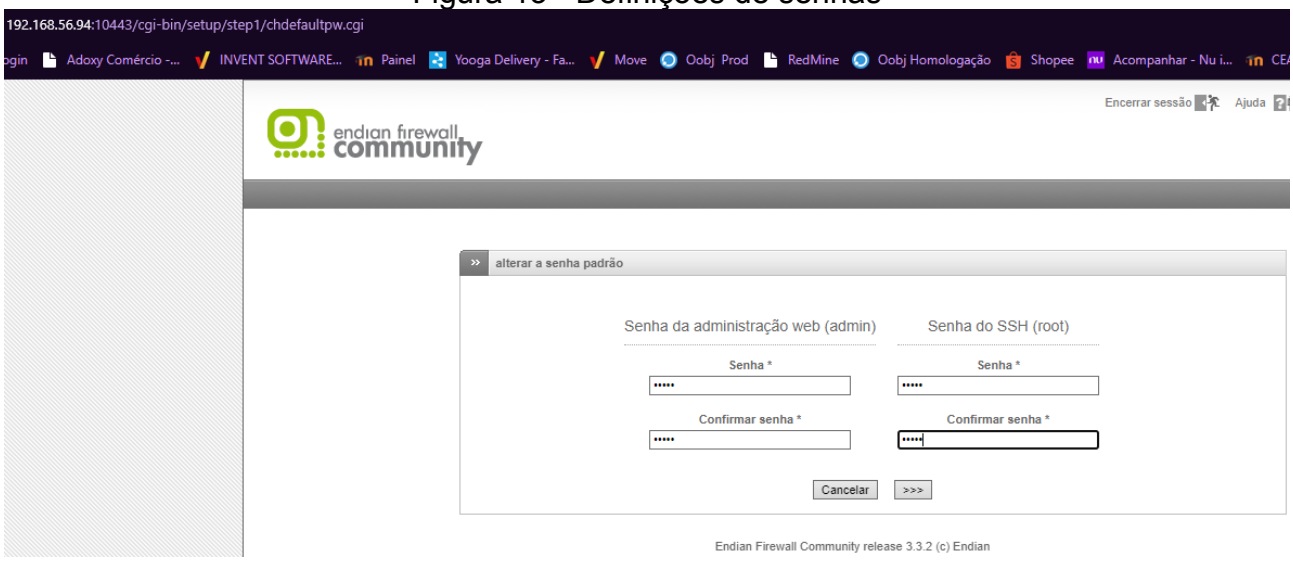


Fonte: autoria própria, 2023

Feita a etapa descrita anteriormente, é mostrada uma mensagem de restauração de *backup*, neste caso, será iniciada uma instalação do zero. A Figura 13 mostra a tela de definições das senhas do portal e servidor.

Após esse processo, se faz uma série de configurações padrões. Um assistente de configuração de rede vai auxiliar, mostrando as configurações de modos de rede, tipo de *UpLink*, configuração da porta vermelha, configuração de rede para a rede verde, na qual será definido o nome do servidor. Além disso, uma possível alteração de endereço e máscara da sub-rede, configuração da rede vermelha, configuração DNS, configuração de *e-mail* do administrador, foram deixadas como padrão. O assistente de configuração é bem intuitivo.

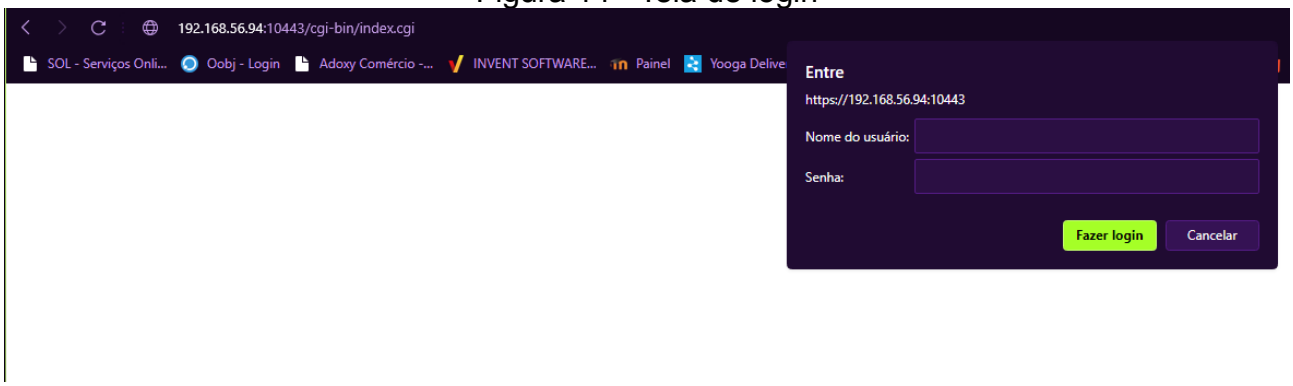
Figura 13 - Definições de senhas



Fonte: autoria própria, 2023

Aplicada as configurações citadas anteriormente, o servidor é reiniciado. Para acessar novamente, o sistema solicita o login e a senha do portal, mostrada na Figura 14.

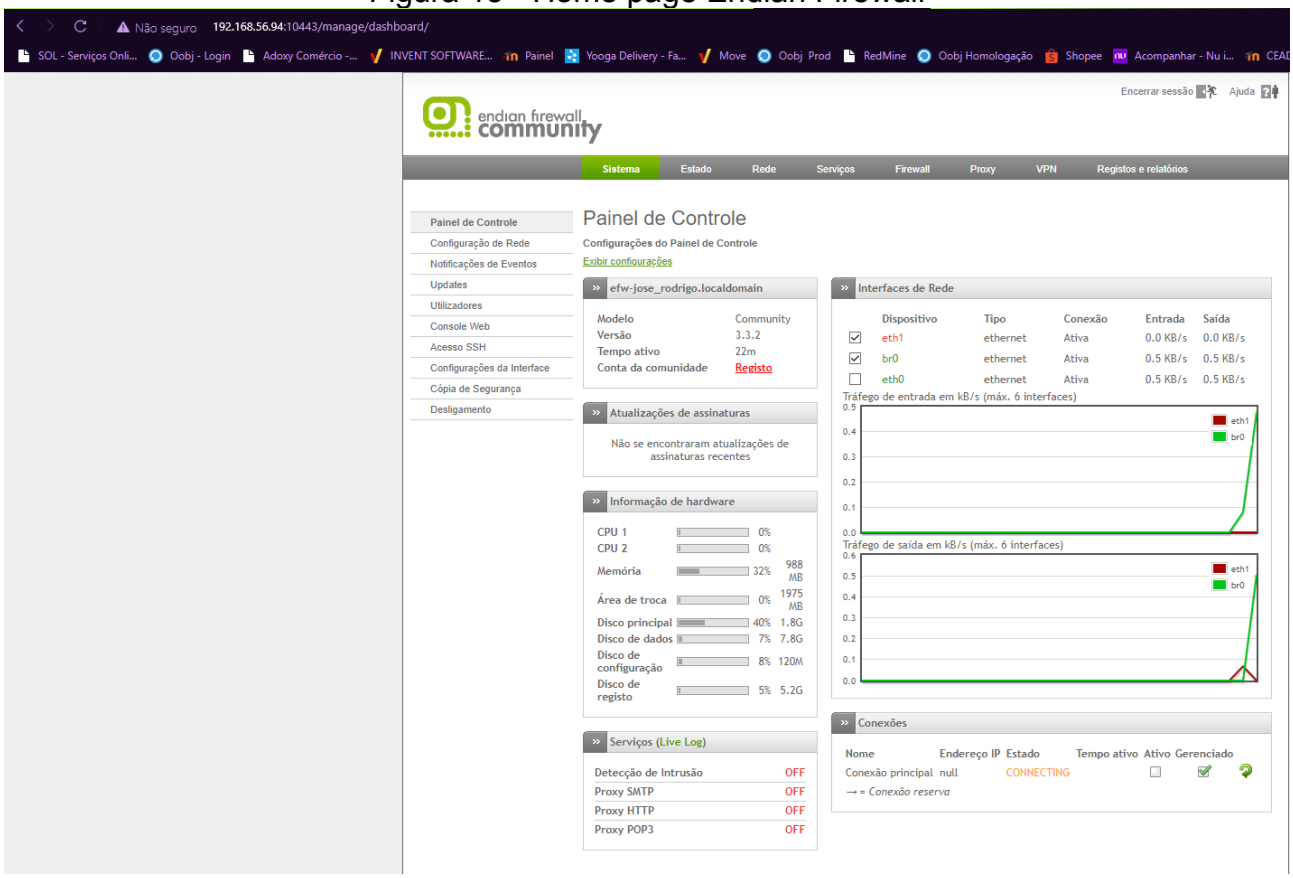
Figura 14 - Tela de login



Fonte: autoria própria, 2023

A tela principal do *Endian* e mostrada na Figura 15. Através dela pode-se acessar todas as possíveis configurações e ‘modelar’ o *software* conforme as necessidades da empresa/residência onde se encontra instalado.

Figura 15 - Home page Endian Firewall



Fonte: autoria própria, 2023

Realizando todos estes passos citados acima, finaliza-se a instalação do *Endian Firewall*.

5 Funções do *Endian Firewal*

Nesse capítulo estão descritas as funcionalidades e como foram realizadas as configurações do *Endian Firewall*. baseadas no material da documentação do *Endian* (2023).

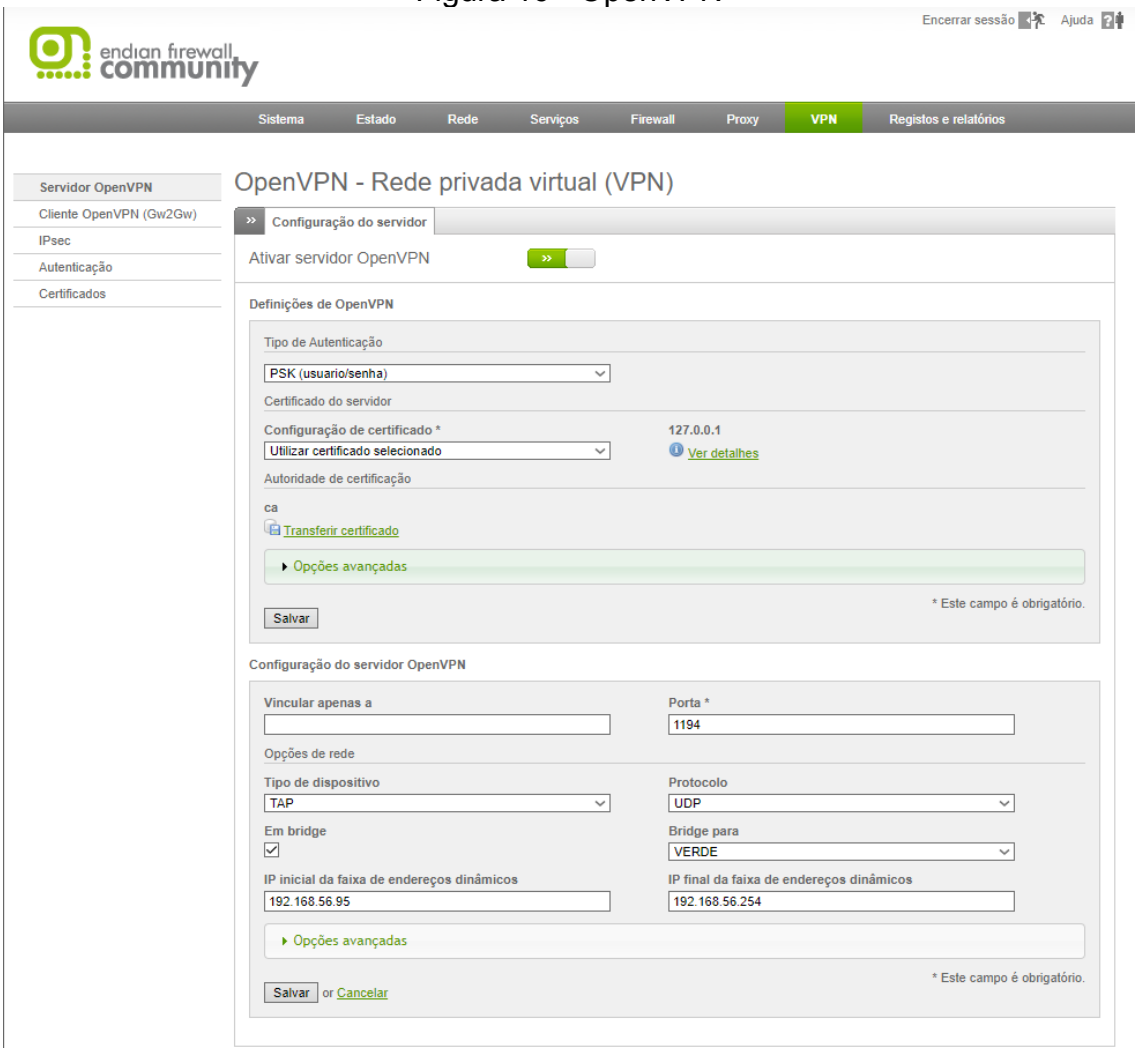
5.1 *Open*VPN *server*

Uma VPN permite que duas redes locais separadas se conectem diretamente entre si por meio de redes potencialmente inseguras, como a Internet. Todo o tráfego de rede através da conexão VPN é transmitido com segurança dentro de um túnel criptografado, escondido. Essa configuração é chamada de VPN *Gateway-to-Gateway* ou, para abreviar, VPN Gw2Gw. Da mesma forma, um único computador remoto em algum lugar da Internet pode usar um túnel VPN para se conectar a uma LAN local confiável. O computador remoto, às vezes chamado de *Road Warrior*, parece estar conectado diretamente à LAN confiável enquanto o túnel VPN está ativo.

Quando configurado como um servidor *OpenVPN*, o *Endian Firewall* pode aceitar conexões remotas do *uplink* e permitir que um cliente VPN seja configurado e interaja com os recursos locais como se fosse uma estação de trabalho ou servidor local.

A página de configurações do servidor *OpenVPN* é composta por uma guia: Configuração do servidor, conforme ilustrado Figura 16.

Figura 16 - OpenVPN



Fonte: autoria própria, 2023

5.2 Firewall

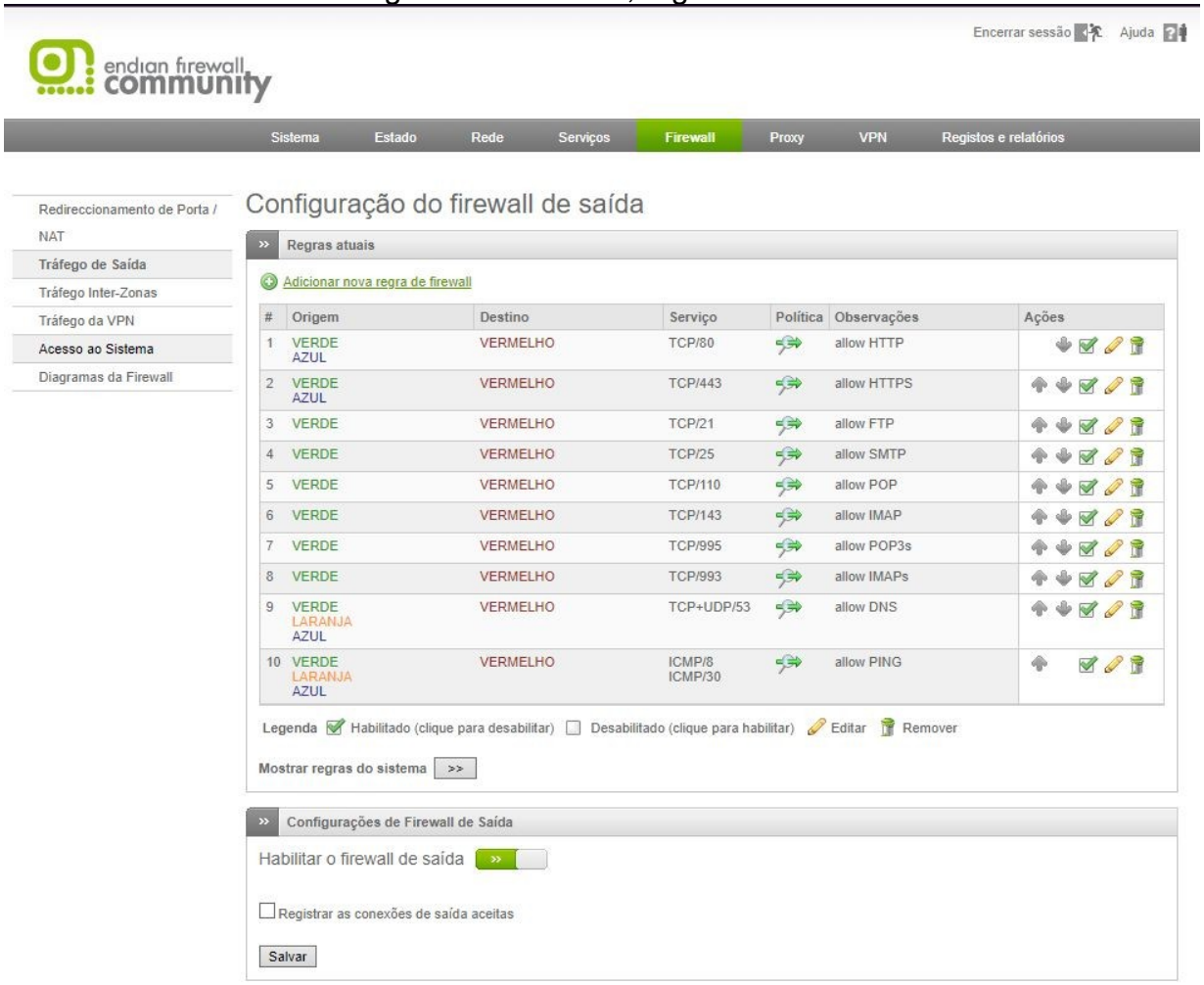
Um *firewall* é um dispositivo de segurança de rede que controla o tráfego, decidindo permitir ou bloquear com base em regras definidas. Essa tecnologia é a linha de defesa primária há mais de 25 anos, estabelecendo uma barreira entre redes internas protegidas e redes externas, como a Internet. *Firewalls* podem ser implementados como hardware, software ou ambos, Cisco Systems, Inc. (2023) .

O *Endian Firewall* vem com um conjunto pré-configurado de regras para o tráfego de saída, para permitir o fluxo de tráfego de serviços, portas e aplicativos específicos das várias zonas para a interface vermelha e, portanto, para a *Internet* . Essas regras são necessárias para garantir que os serviços mais comuns sempre possam acessar a Internet e funcionar corretamente.

É possível desabilitar ou habilitar todo o *firewall* de saída clicando no botão Desabilitado trocar. Quando desabilitado, todo o tráfego de saída é permitido e nenhum pacote é filtrado: No entanto, essa configuração é fortemente desencorajada e a recomendação é manter o *firewall* de saída ativado.

A Figura 17 apresenta a tela inicial do *firewall* cuja qual não iremos nos aprofundar nesse momento.

Figura 17 - Firewall, regra de saída



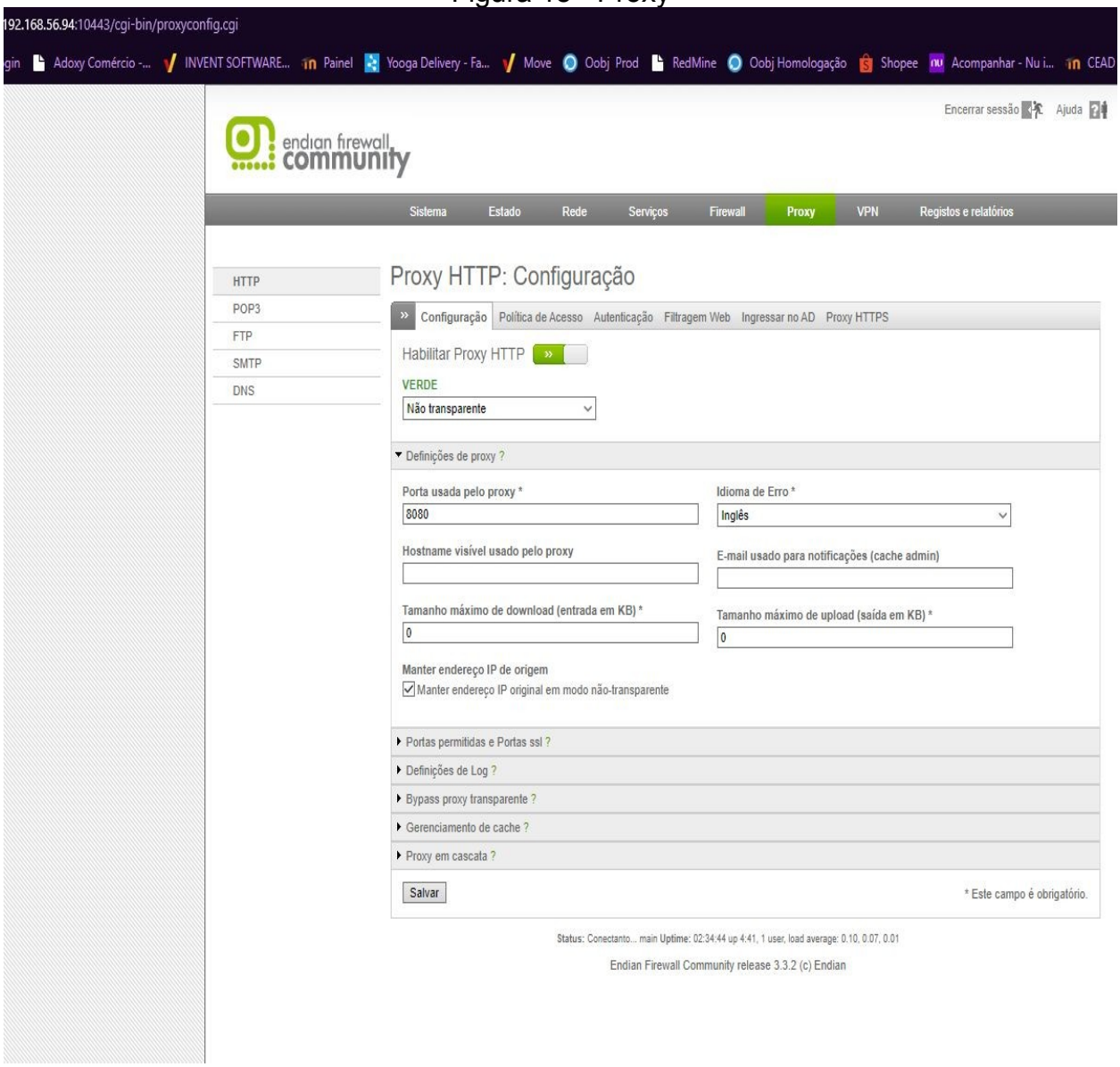
Fonte: autoria própria, 2023

5.3 Proxy

Um servidor *proxy* é um sistema, localizado entre um cliente (que solicita uma página da web ou algum recurso) e as redes externas com o objetivo de capturar todas as solicitações do cliente, recuperar os recursos solicitados e transmiti-los ao cliente. A principal vantagem de um servidor *proxy* é sua capacidade de armazenar em cache (ou seja, armazenar localmente) todas as páginas solicitadas, tornando mais rápidas as

solicitações futuras das mesmas páginas. A Figura 18 apresenta a tela inicial do *Proxy* presente no *Endian Firewall*

Figura 18 - Proxy

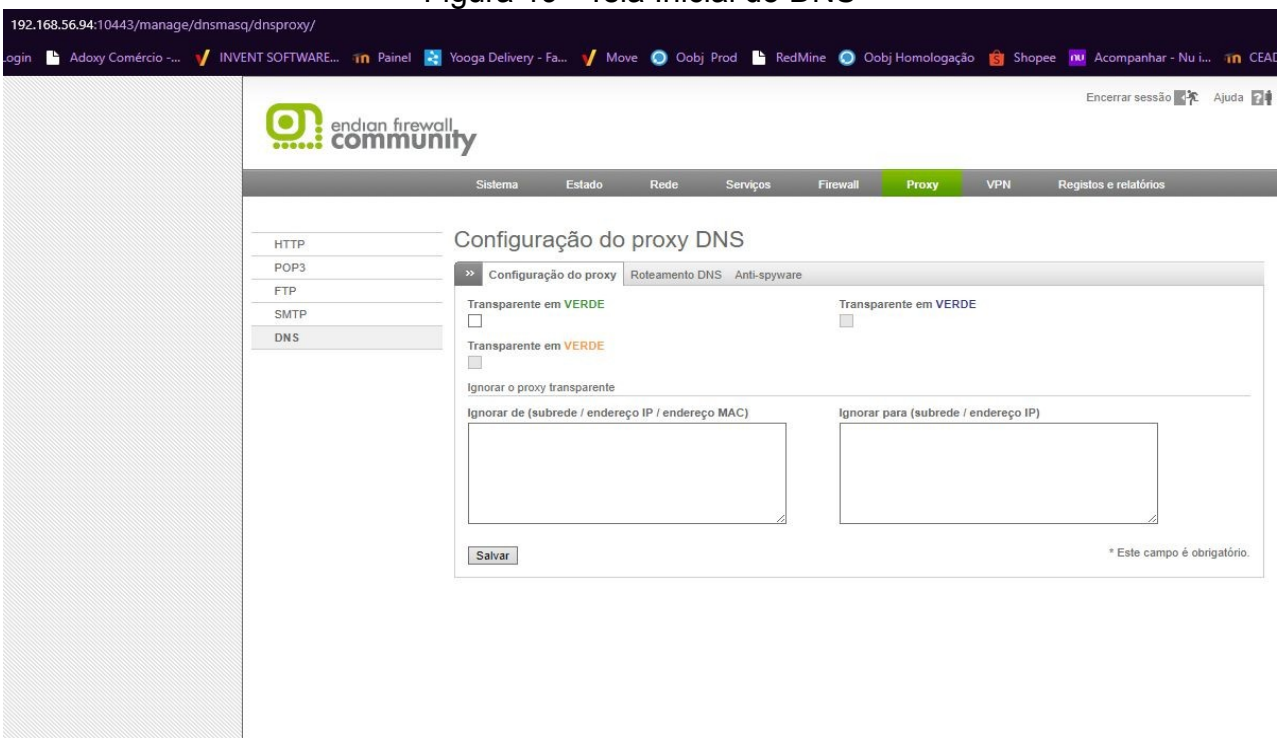


Fonte: autoria própria, 2023

5.3.1 DNS

O *proxy* DNS é um servidor *proxy* que intercepta consultas DNS e as responde, sem a necessidade de contatar um servidor DNS remoto cada vez que for necessário resolver um endereço IP ou um nome de *host*. Quando uma mesma consulta é frequentemente repetida, armazenar em cache seus resultados localmente pode melhorar sensivelmente o desempenho. As configurações disponíveis para o *proxy* DNS são agrupadas em três páginas. Na figura 19 é mostrada a tela do DNS do *Endian*.

Figura 19 - Tela Inicial do DNS



Fonte: autoria própria, 2023

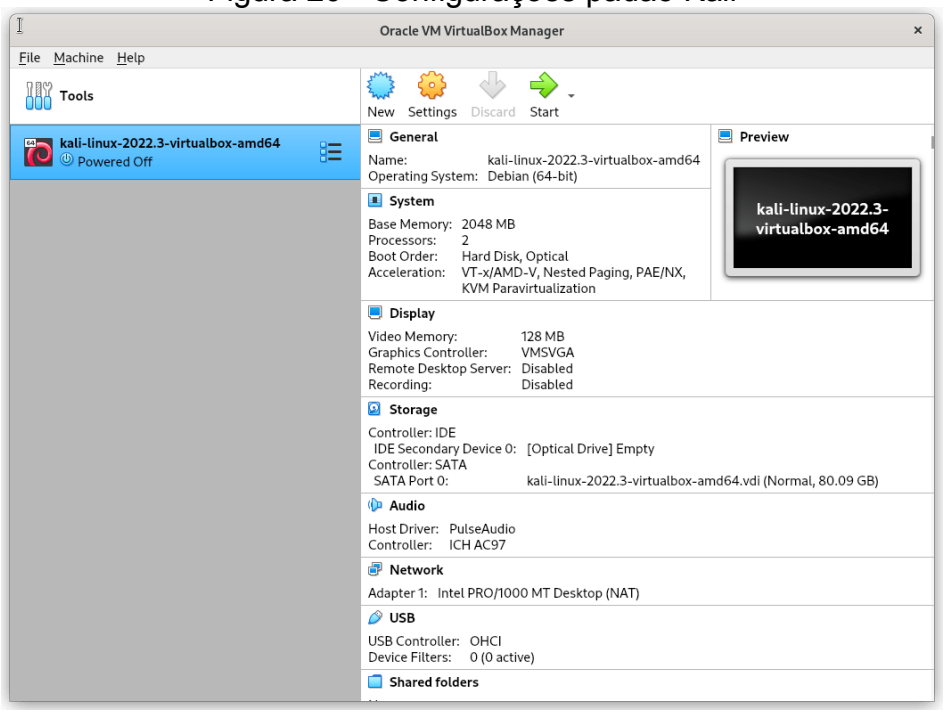
6 EXPERIMENTOS

Nesta seção serão executadas as funcionalidades: *OpenVpn, Proxy* e *Firewall* do *Endian*, para avaliação e validação dessas.

6.1 Instalação Kali Linux

Para instalação do *Kali Linux*, foi usada um versão que o próprio site disponibiliz para VMs, necessário apenas extrair é instalar ele. Porém se fosse preciso fazer a instalação do zero, esses são os requisitos: 128 MB de RAM (512 MB recomendado) e 2 GB de espaço em disco se nenhuma interface gráfica for usada. 2 GB de RAM e 20 GB de espaço em disco com área de trabalho e coleção de pacotes por padrão. Pelo menos 8 GB de RAM para os aplicativos que exigem mais recursos, Gonzalez (2022). A configuração está Ilustrado pela Figura 20.

Figura 20 - Configurações padão Kali



Fonte: Kali, 2023

Única alteração sofrida nessa configuração foi a configuração de rede, sendo ajustada para ficar na igual a do *Endian*, *Host Only*, acatando as configurações do *software* de segurança.

6.2 Proxy

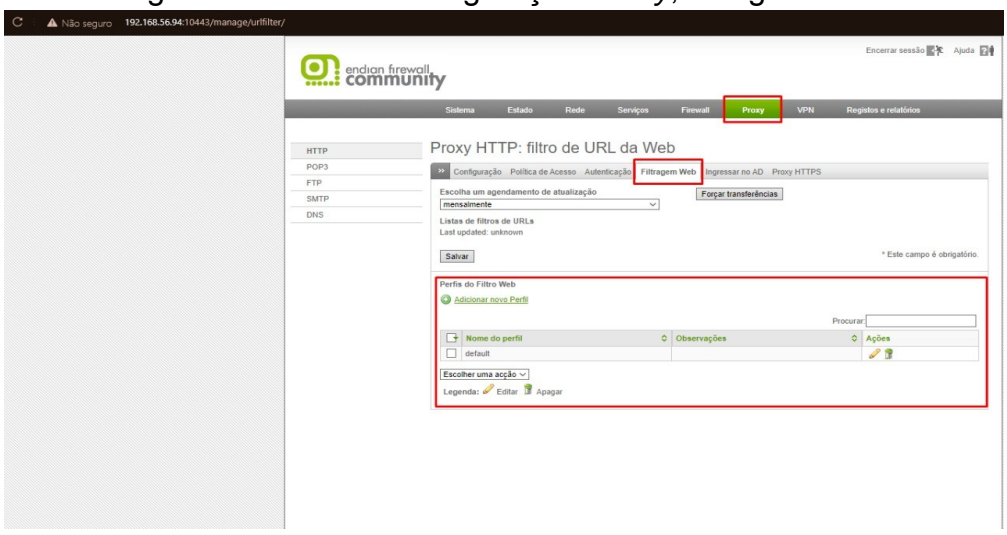
O *Proxy* detém uma das mais importantes funções dentro deste software, sendo capaz de filtrar palavras e sites.

6.2.1 BLOQUEAR SITES

Nesse experimento foi validado a função do software de bloquear acesso a sites.

Dentro da tela de configuração do software, na aba *Proxy*, existem duas opções, as duas são validas, primeira configuração, HTTP, Filtragem Web, configuração de perfil, conforme mostrado na Figura 21.

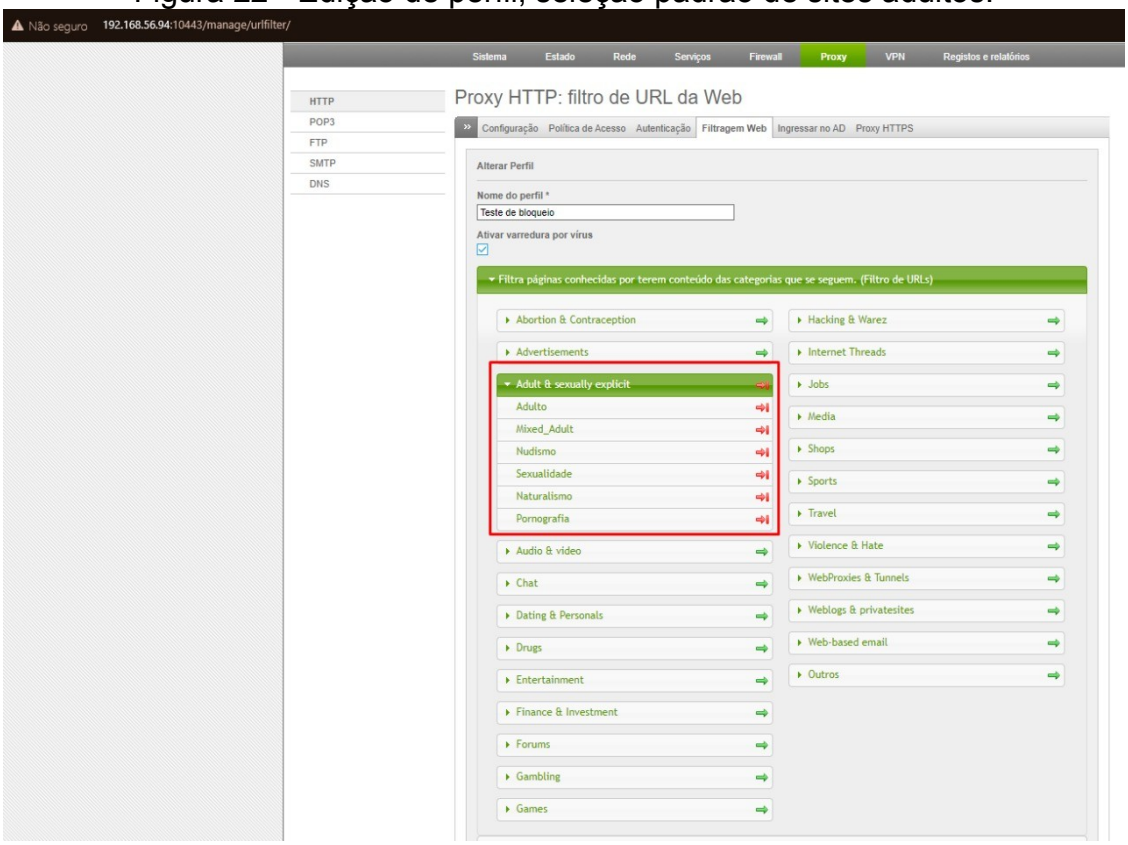
Figura 21 - Tela de configuração *Proxy*, filtragem *Web*



Fonte: autoria própria, 2023

Dentro dessa tela será exibido uma configuração de perfil, bem como de seleção, cada perfil e configurável, usado como exemplo o perfil padrão, dentro de sua configuração foi habilitado '*Adult & security explicity*', quando habilitado será realizado uma filtragem de sites adultos e nudez, impedindo qualquer acesso a sites com esse teor, porém existem mais configurações, que podem ser seguidas a gosto do administrador. Tela de configuração, ilustrado pela Figura 22.

Figura 22 - Edição de perfil, seleção padrão de sites adultos.

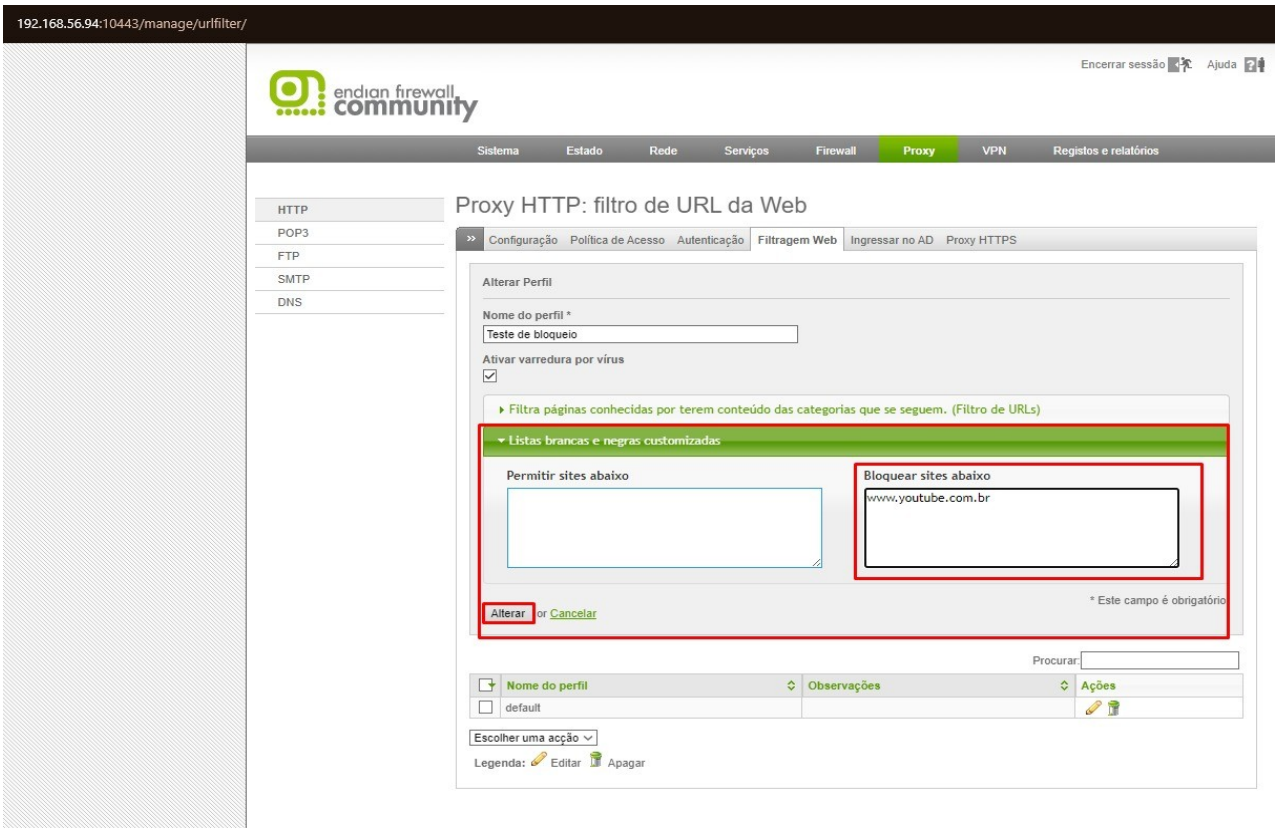


Fonte: autoria própria, 2023

A configuração seguinte foi especifica para um site. Basta acessar as caixas definidas nas configurações, a caixa da esquerda é realizada a configuração de permitir acesso. O site ou domínio especificado, será único que poderá ser acessado. O contrario ocorre na caixa da direita, especificando um site/domínio nela, este será bloqueado, enquanto o resto permanece ativo.

A configuração pode ser aplicado, restringindo mais ainda o acesso, permitindo apenas acesso à um domínio especifico ou barrando sites específicos. Configuração muito útil tanto em empresas como para controle parental em residências. Exemplo da configuração na Figura 23.

Figura 23 - Configuração especifica de site

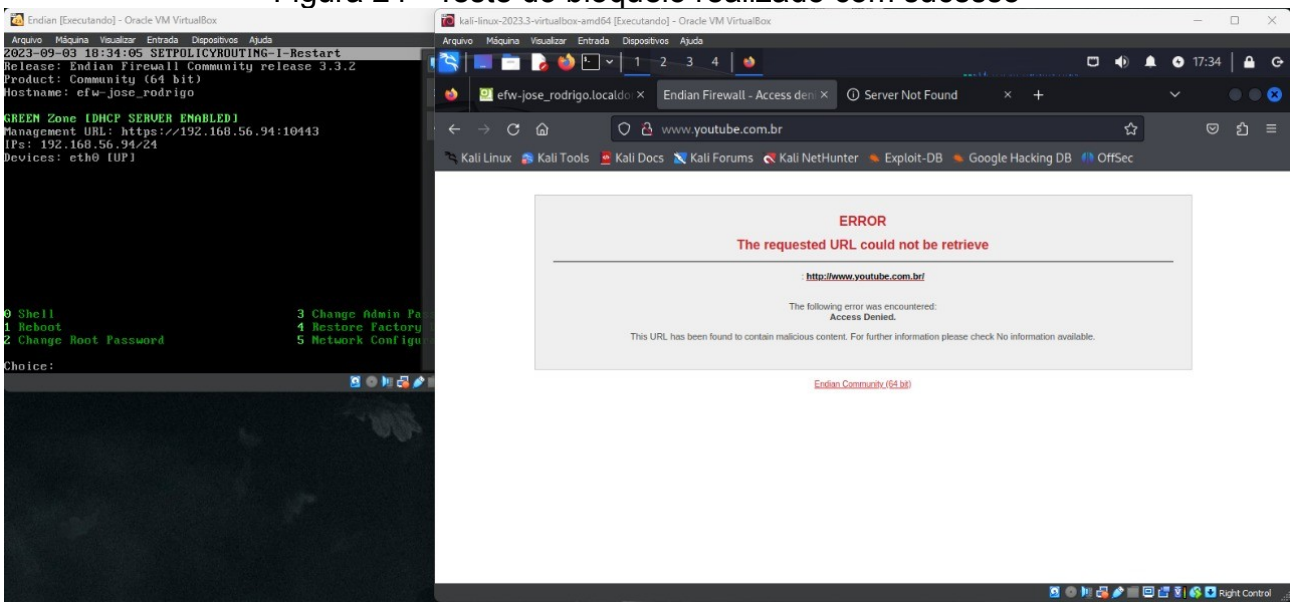


Fonte: autoria própria, 2023

Realizadas as devidas configurações, primeiro teste realizado com sucesso, a maquina virtual do Kali foi inicializada, o navegador *FireFox* foi acessado, digitado o domínio configurado, bloqueio realizado conforme esperado.

Na Figura24 está o servidor do *Software Endian* do lado esquerdo e Kali do lado direto, demostrando o bloqueio.

Figura 24 - Teste do bloqueio realizado com sucesso



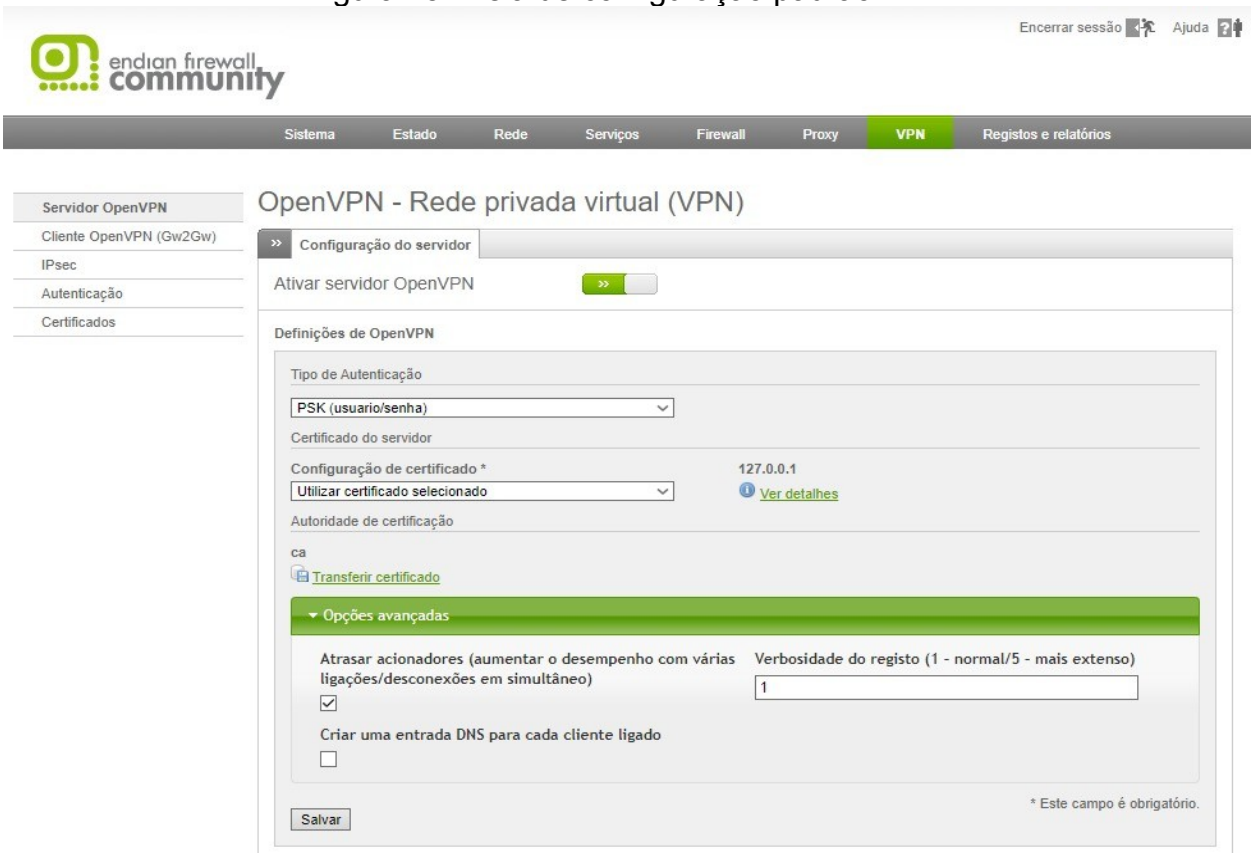
Fonte: autoria própria, 2023

Mesmo realizando as configurações de bloqueios, ambos são facilmente burlados instalando uma VPN, que pode ser gratuita ou paga. Até mesmo as versões presentes em navegador é possível ultrapassar este bloqueio.

6.3 Open VPN

Dentro da tela do monitor, acessando a aba responsável pelo VPN, é realizado o ligamento do servidor. Servidor habilitado, será preservado as configurações padrões. Tipo de chave, PSK (chave, usuário), usar o certificado padrão, disponibilizado pelo próprio *Endian*. Conforme mostra a Figura 25.

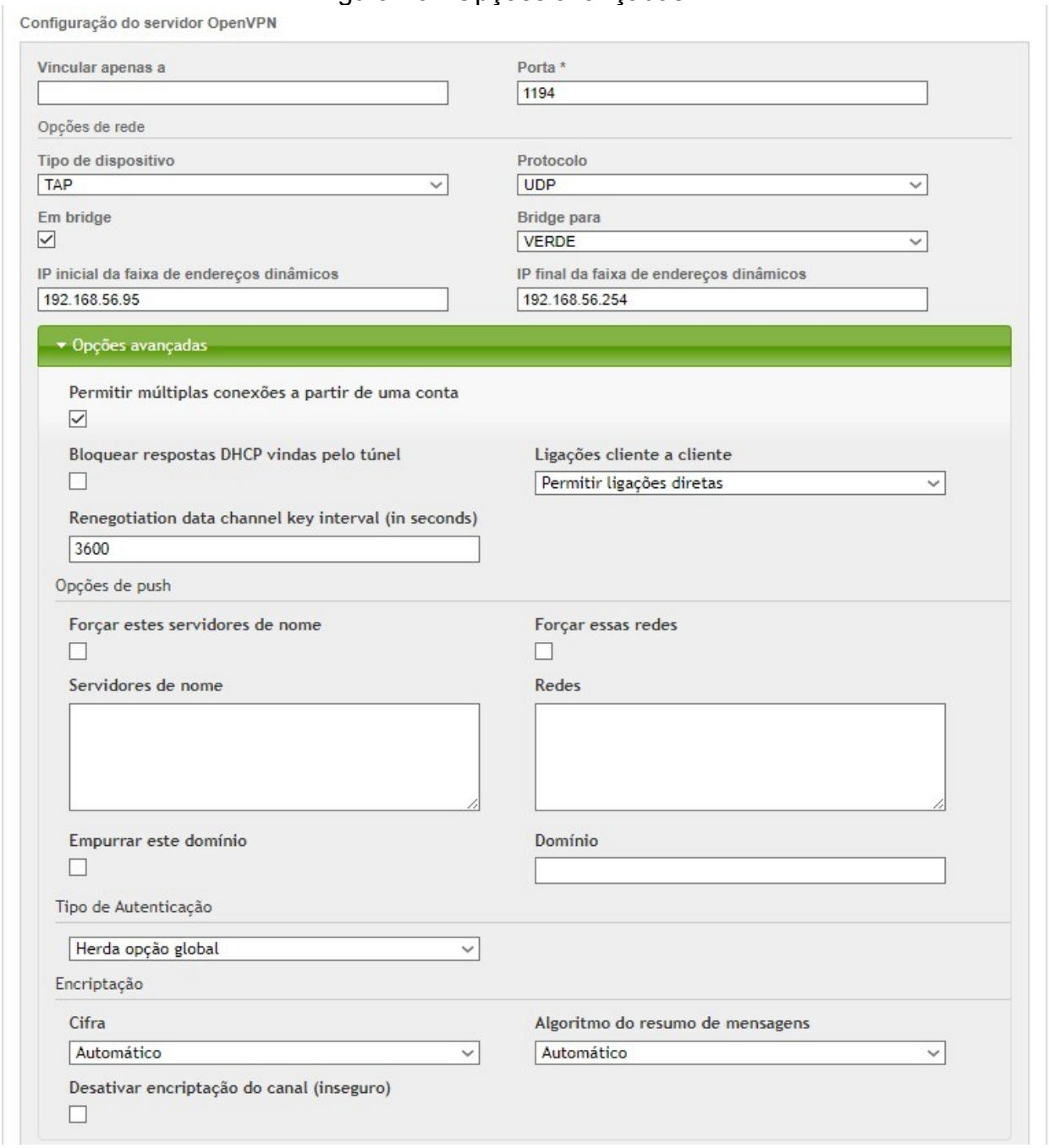
Figura 25 - Tela de configuração padrão VPN



Fonte: autoria própria, 2023

O próximo passo, é apresentada uma configuração a mais, a configuração do servidor em si. Também é preservada a configuração padrão, exceto por “Permitir múltiplas conexões”. Como o nome já descreve, vai permitir mais de um cliente se conectar ao ambiente ao mesmo tempo. Opções avançadas VPN estão mostradas na Figura 26.

Figura 26 - Opções avançadas VPN



Fonte: autoria própria, 2023

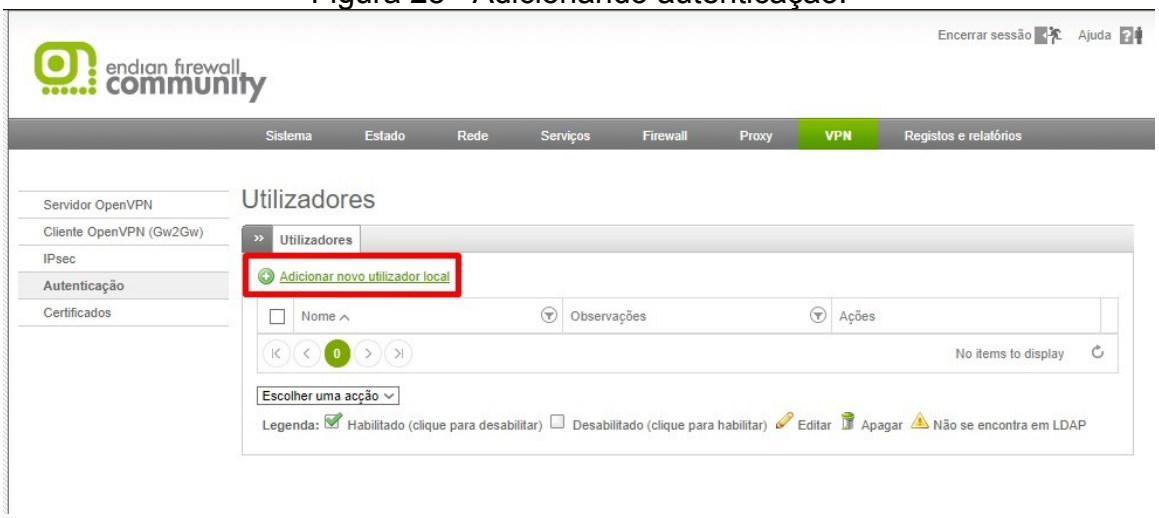
Realizado o passo anterior, faz-se o *download* do certificado. Este certificado vai ser usado na configuração do cliente, que vai realizar o túnel com servidor, ou seja, o acesso direto. O download do certificado está mostrado na Figura 27.

Figura 27 - Download do certicado.

Fonte: autoria própria, 2023

A autenticação, será definida como vai ocorrer no passo seguinte. Ainda na aba do VPN, selecionando autenticação, adicionar novo utilizado local, ilustrado na Figura 28.

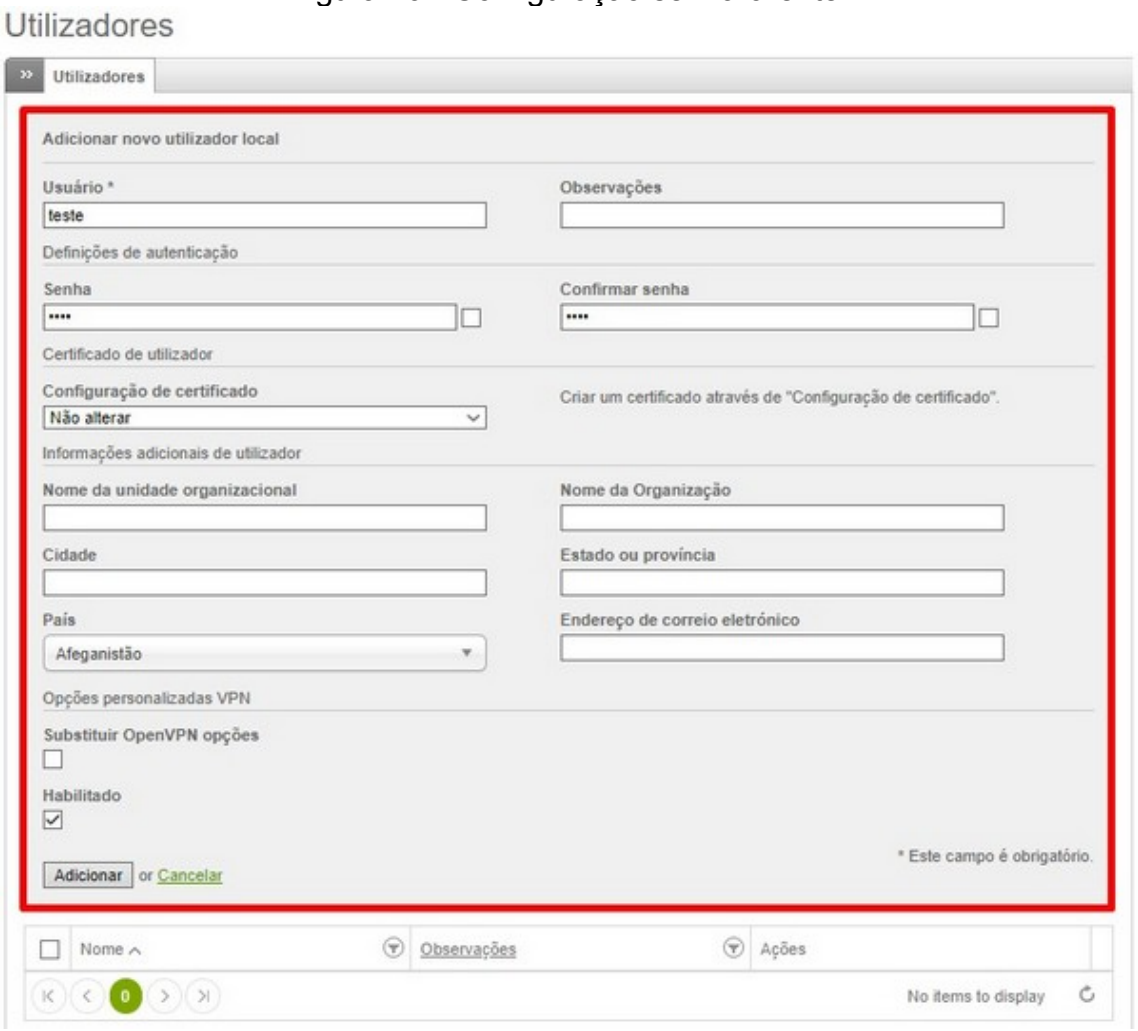
Figura 28 - Adicionando autenticação.



Fonte: autoria própria, 2023

Na próxima tela vai ser informado os dados com os quais o cliente vai utilizar para acessar o sistema, usuário e senha, conforme mostrado na Figura 29.

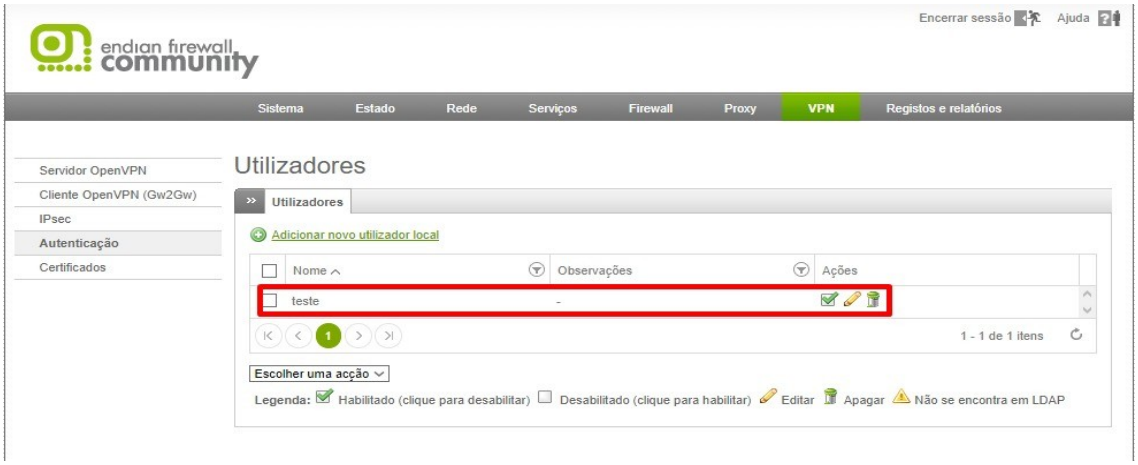
Figura 29 - Configuração senha cliente.



Fonte: autoria própria, 2023

Para salvar a configuração anterior, basta clicar no botão adicionar, em seguida será possível visualizar o utilizador, que futuramente tera acesso ao servidor, todo o processo de criação de login e senha, é realizada internamente, diretamente no cliente. Perfil recém criado, conforme tela mostrada na Figura 30.

Figura 30 - Perfil criado.



Fonte: autoria própria, 2023

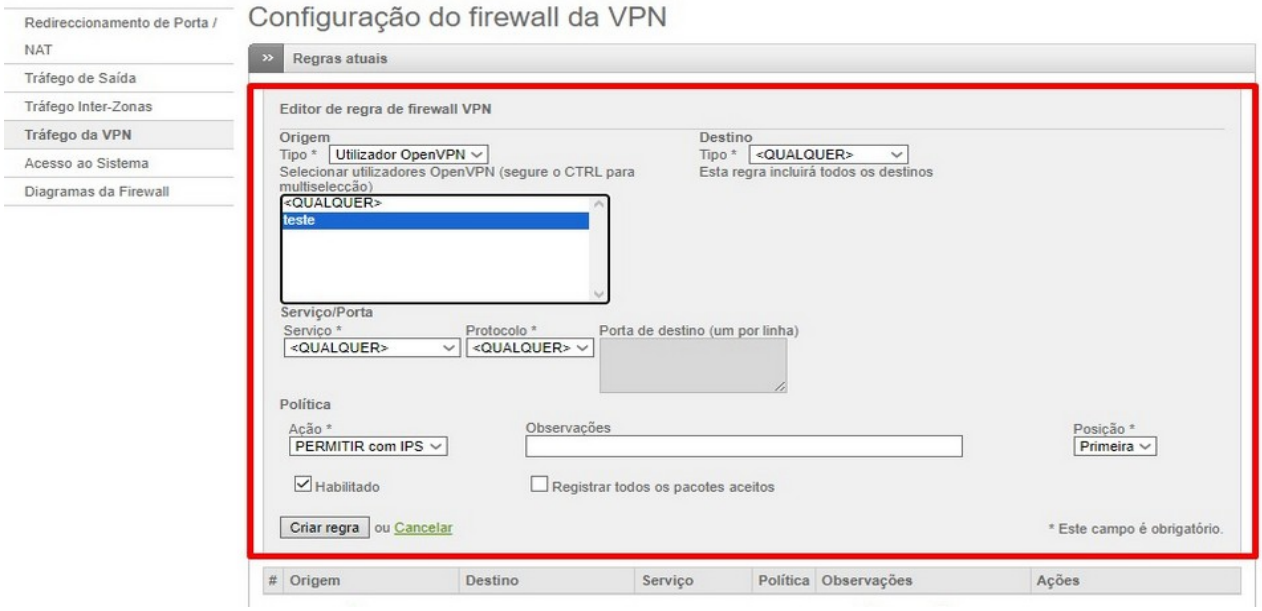
Agora, com o perfil de VPN pronto, acessar a aba *Firewall*, configuração de tráfego de rede. Na qual será criado uma regra especifica para que o login ocorra sem problemas, acessando “Adicionar nova regra de *Firewall* VPN”, conforme mostrado Figura 31.

Figura 31 - Tráfego VPN

Fonte: autoria própria, 2023

Dentro do editor de regra do *Firewall*, o tipo origem utilizado nessa configuração será “Utilizado Open VPN”, e o tipo Destino “Qualquer”, isso significa, que nessa configuração, qualquer maquina, pode acessar esse Open VPN. Serviço e porta, também não foi especificado, tornando mais simples o acesso, ação “Permitir com IPS (*In-Plane Switching*)”, com essa configura ativa, ele realiza uma validação a mais, vai verificar a regra junto ao *Intrusion Protocol*, conforme ilustrado na Figura 32.

Figura 32 - Configuração trafego VPN



Fonte: autoria própria, 2023

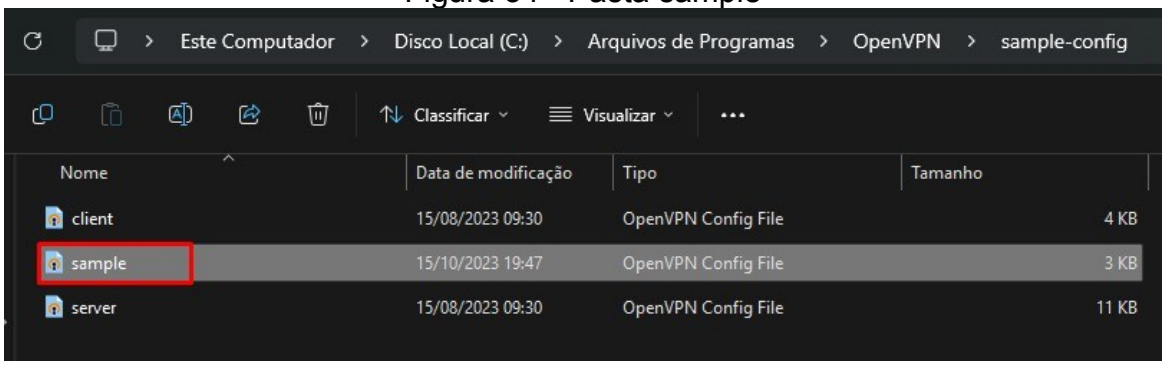
Com a configuração realizada, apenas clique em criar nova regra,e a configuração será salva, a seguinte tela será apresentada, conforme mostra a Figura 33.

Figura 33 - Salvando configuração de tráfego.

Fonte: autoria própria, 2023

Fazendo as configurações dentro dos arquivos *OpenVPN* instalados no aplicativo cliente. Acessando o local dos arquivos, primeiro é feita adição do arquivo chamado "*sample*" com a extensão .ovpn. Nas versões mais atuais do cliente, quando feito o download esse arquivo não vem junto. O arquivo e mostrado dentro da pasta "sample-config", conforme mostrado na Figura 34.

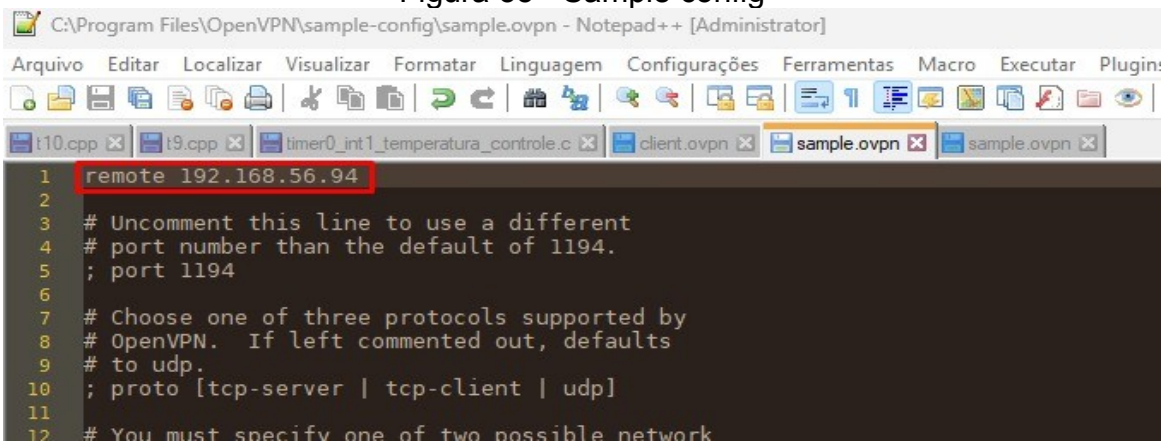
Figura 34 - Pasta sample



Fonte: autoria própria, 2023

Esse arquivo foi colhido no próprio site da *OpenVPN*, vem com as configurações padrões. Sendo assim, é necessário fazer a configuração dele, acessando o arquivo com um programa de edição de texto qualquer, nesse caso foi usado o *NotePad++*, é colocado apenas o endereço do servidor do *Endian*, conforme ilustrado pela Figura 35.

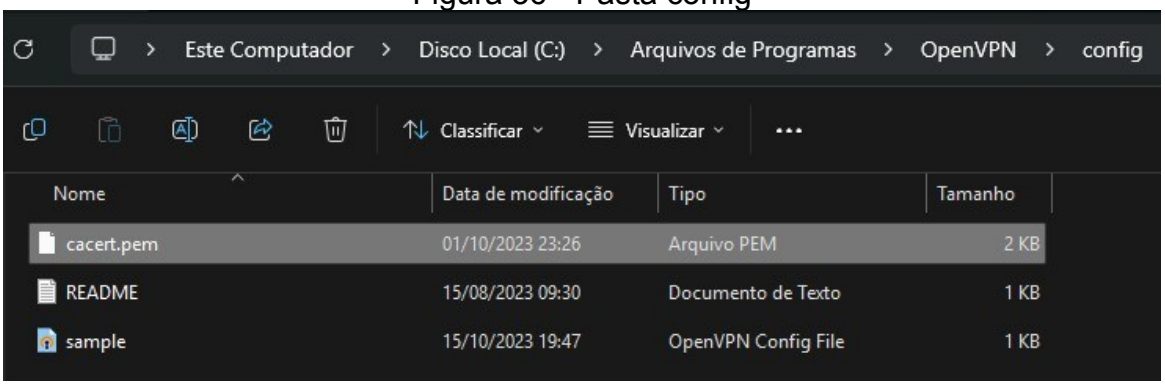
Figura 35 - Sample config



Fonte: autoria própria, 2023

Outro arquivo com o mesmo nome deve ser adicionado. Dessa vez a pasta na qual o arquivo vai ser colocado se chama “config”. Ainda nessa pasta será colocado o certificado baixado nos passos anteriores. Ilustrado pela Figura 36, consta o arquivo “sample” e o certificado “cacert.pem”.

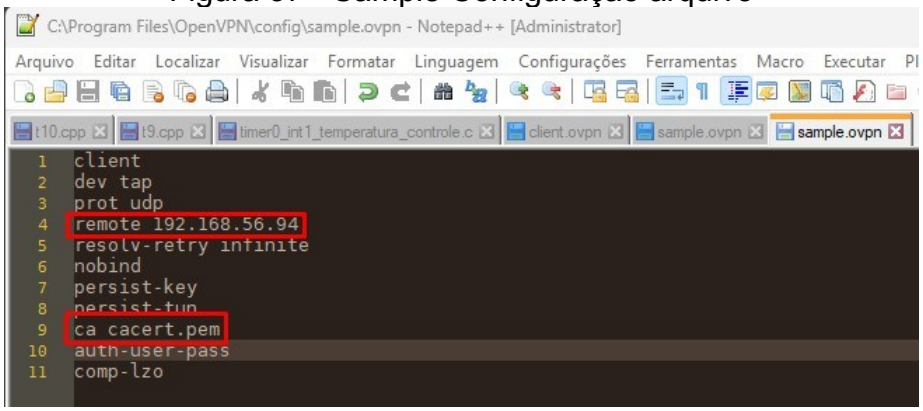
Figura 36 - Pasta config



Fonte: autoria própria, 2023

Acessando o arquivo “sample” das pasta “config” com o editor de texto, é feita a seguinte configuração. É definido o endereço remoto, no qual ele vai realizar a conexão, também apontado o nome do certificado. Esse arquivo também foi colhido no site *OpenVPN.* conforme mostrado pela Figura 37.

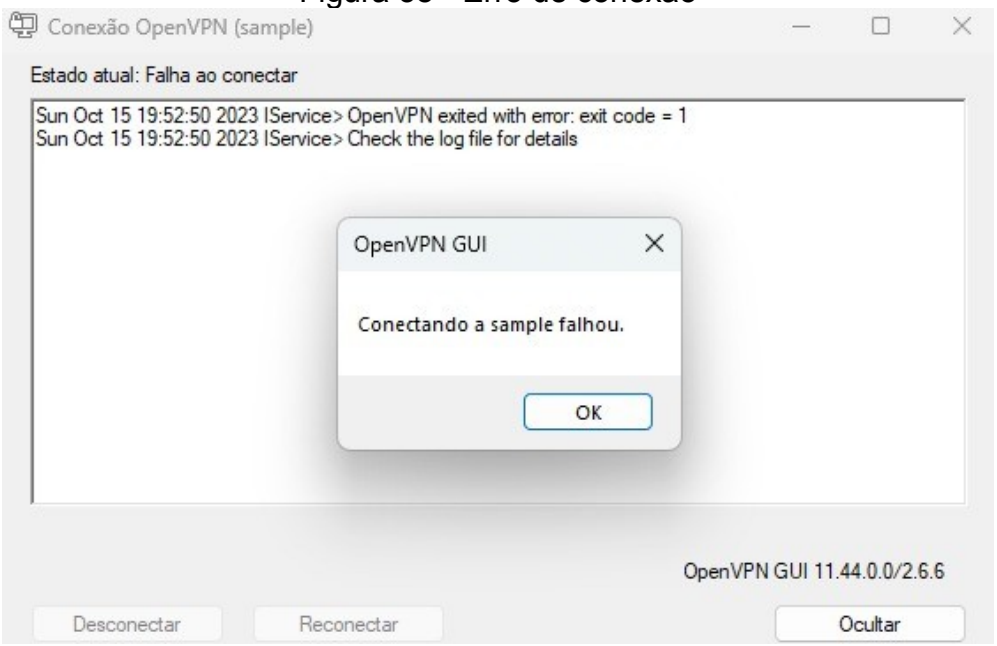
Figura 37 - Sample Configuração arquivo



Fonte: autoria própria, 2023

Sobre o teste realizado, devido a escolha de rede interna, não foi possível fazer o “túnel” da VPN funcionar. Acessando de uma maquina externa, erro ilustrado pela Figura 38.

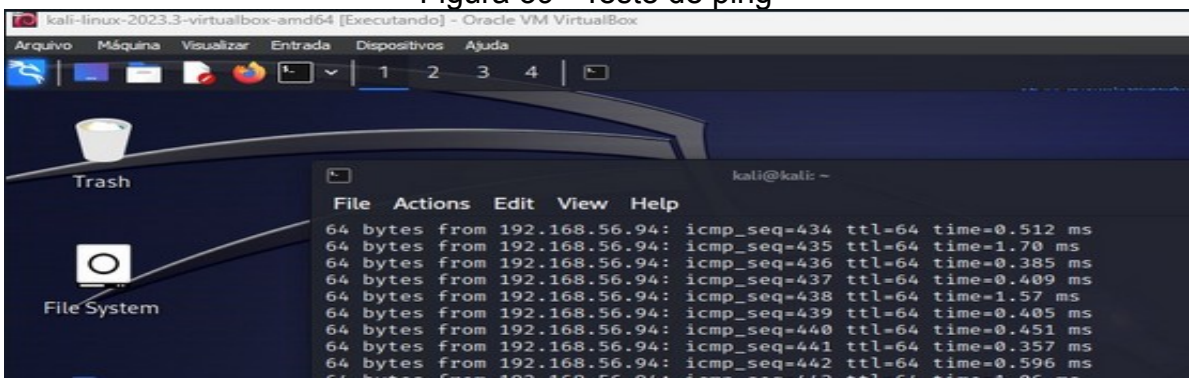
Figura 38 - Erro de conexão



Fonte: autoria própria, 2023

Usando a mesma configuração, porém da maquina hospeda na mesma rede a conexão foi realizada com sucesso. Essa configuração é muito usada para acessar uma área de trabalho de remoto, colocando uma regra na qual só pode ser acessado se estiver logado em tal rede. Figura 39 mostra um teste de ping no IP do servidor do *Endian.*

Figura 39 - Teste de ping



Fonte: autoria própria, 2023

6.4 Firewall

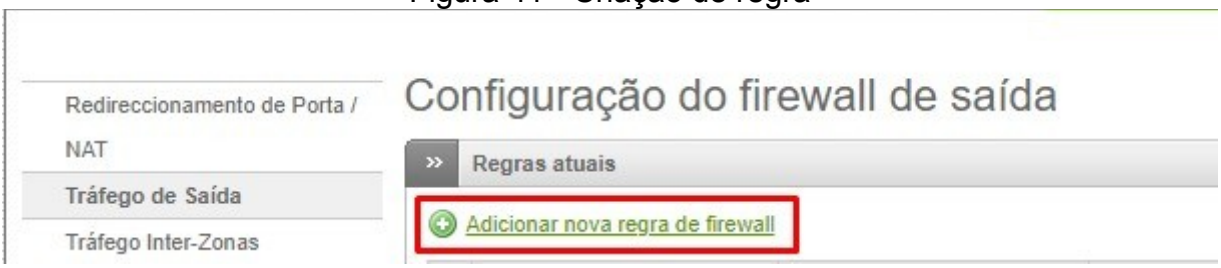
A configuração da regra de saída vai permitir controlar o fluxo. Por padrão, o *Endian* já possui algumas regras, tais como: HTTP, HTTPS, DNS e etc, conforme ilustrado pela Figura 40. Cada regra fica localizada em uma linha, mostrando uma série de informações a respeito, destinação, serviço e porta, por exemplo.

Figura 40 - Regra de saída

Fonte: autoria própria, 2023

Criação de regra Serviço de Compartilhamento de arquivos, ou *Server Message Block* (SMB). O SMB permite que outra maquina acesse os seus arquivos, crie, edite, salve e delete. Vai depender do administrador dessa rede. A tela de configuração de regra de saída, vai exibir um link para criação de um nova regra, mostrado na Figura 41.

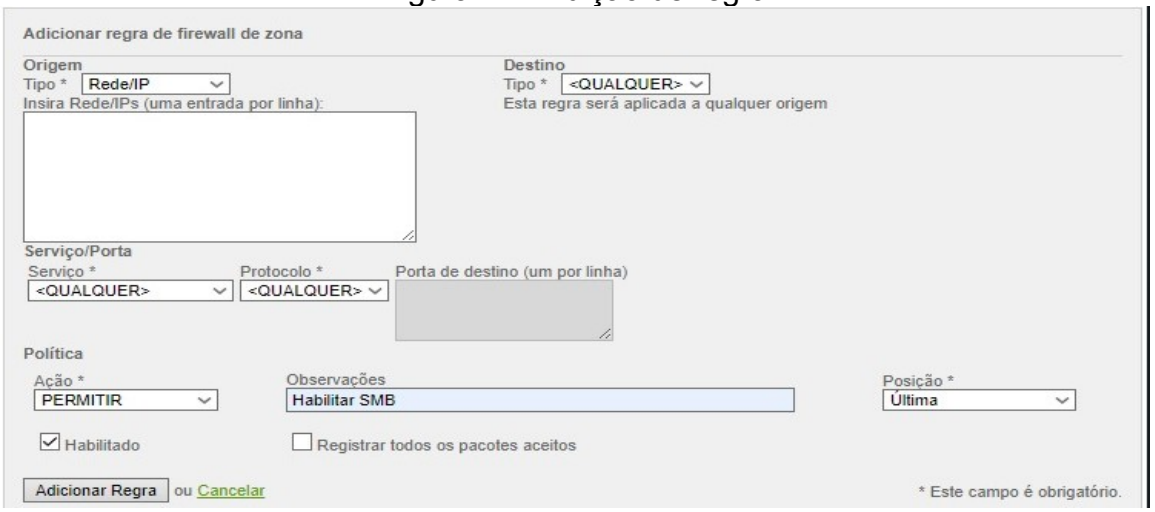
Figura 41 - Criação de regra



Fonte: autoria própria, 2023

Depois disso serão exibidas as configurações para criação da regra. O tipo origem informa o tipo de regra que vai ser respeitada para a acessar a rede interna. Deixado como “Rede/IP”. Tipo destino, que vai receber as informações e acesso, será configurado como qualquer, basta que a maquina esteja conectada na mesma rede. Politica, define se será permitido ou não. Serviço e protocolo, informado o tipo de serviço, exemplo SMB, protocolo, a porta. Deixado com a configuração padrão, conforme Figura 42.

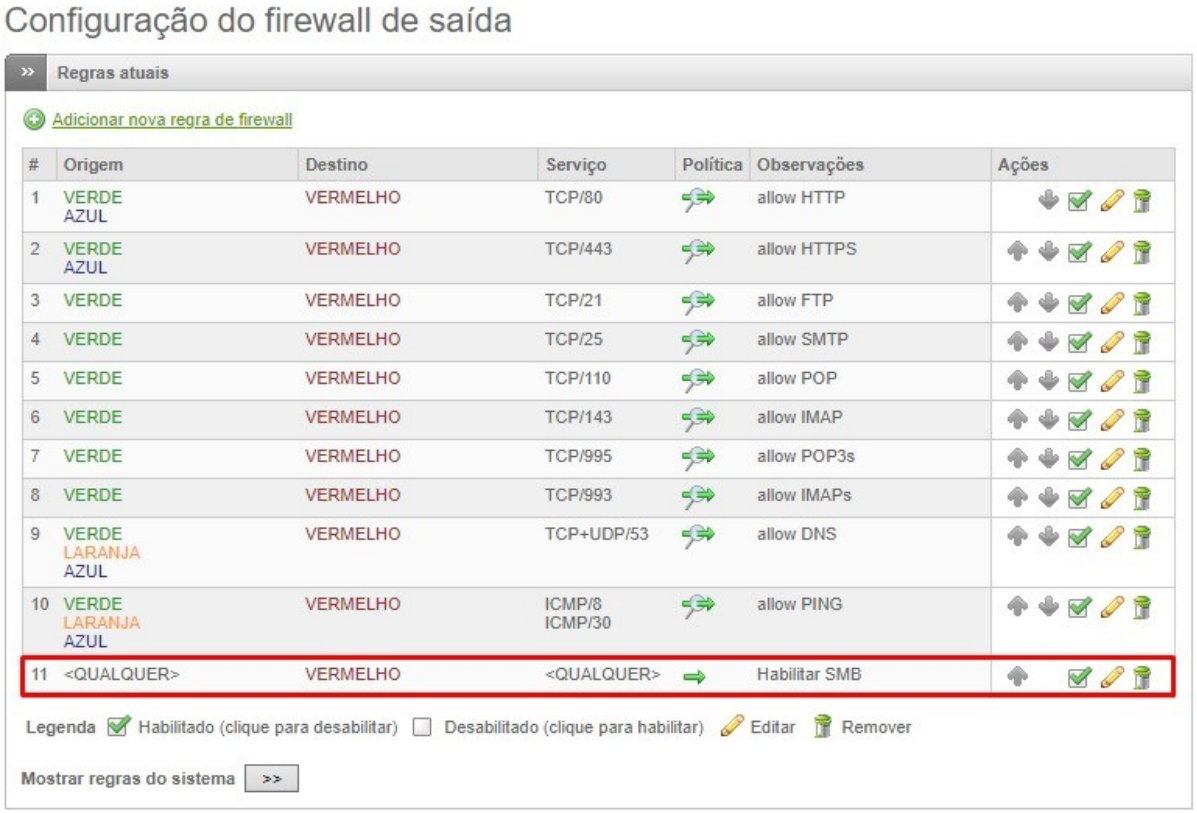
Figura 42 - Adição de regra



Fonte: autoria própria, 2023

Feita a adição da regra, será exibido da seguinte maneira, conforme mostrado na Figura 43.

Figura 43 - Exibição da nova regra



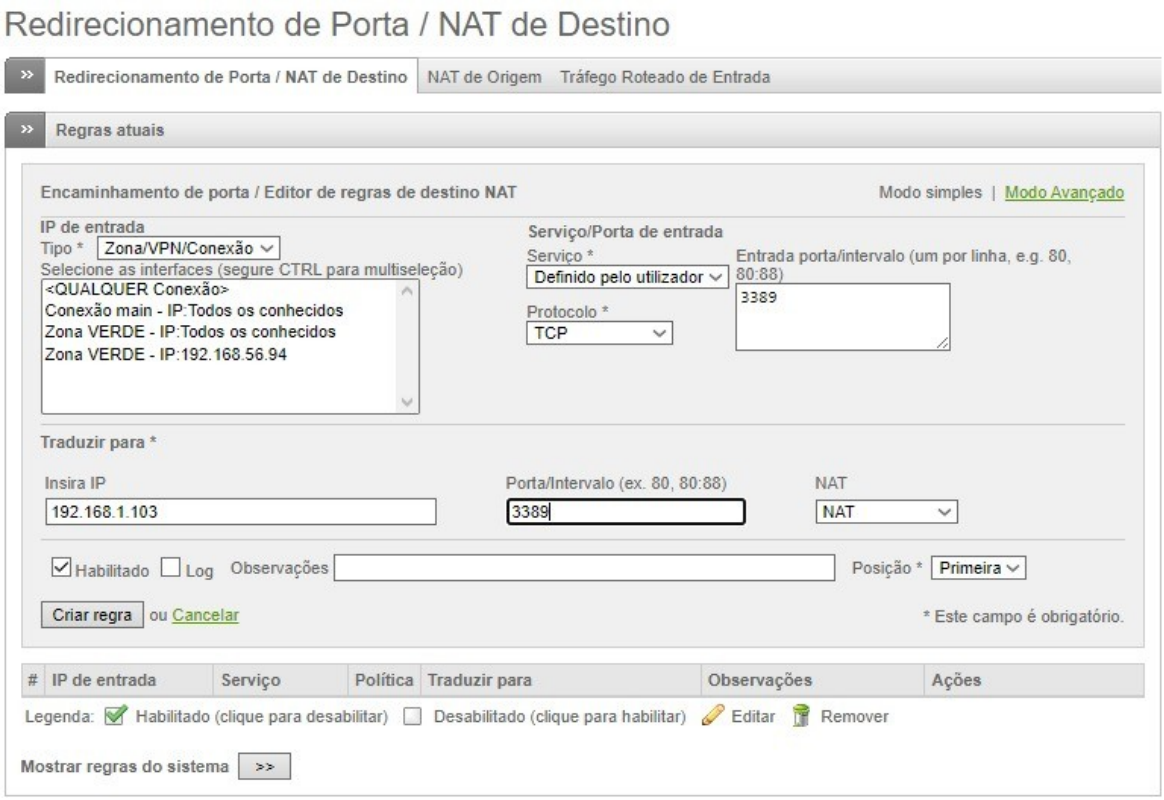
Fonte: autoria própria, 2023

Com essa configuração ativa, qualquer computador logado na mesma rede vai acessar os arquivos de outra máquina. Se alterada ou informada mais algum requisito, será respeitado conforme definido.

Redirecionamento da porta/Nat de Destino, tráfego que vem da Internet com destino a rede interna - essa opção tem várias finalidades, será simulada uma configuração que permite acesso de uma área de trabalho remoto. Na configuração de redirecionamento de porta, é criado uma nova regra IP de entrada. O IP que vai realizar a conexão é usado o tipo “Zona/VPN/Conexão”, que vai exibir quatro tipos de conexões. Será usado “AnyUPlink”, ou seja, qualquer tipo. A configuração do *Endian* não exibe a área de trabalho remota. Foi usado “Definido pelo utilizador”. O protocolo, usado o TCP, porta 3389, porta padrão usada pela aplicação de área de trabalho remoto. “Traduzido

para” é o nome do botão da configuração, aponta o IP que vai receber as conexões de fora. A porta preservada foi a anterior, ou seja, a 3389 e o NAT também foi preservado NAT, conforme mostrado na Figura 44.

Figura 44 - Redirecionamento de Porta/Nat de destino



Fonte: autoria própria, 2023

Realizada estas definições, basta criar a regra. Ainda nessa regra, é possível adicionar para que sempre salve um log das conexões. Isso é uma ferramenta interessante, sendo possível verificar todas as atividades de conexões.

Com essa configuração ativa, qualquer solicitação de acesso feita de fora da rede será direcionada para o IP informado na configuração. Essa configuração pode sofrer várias alterações e se tornar ainda mais rígida, conforme as demandas do administrador. Regra criada, ilustrada na Figura 45.

Figura 45 - Salvamento da regra Nat

Fonte: autoria própria, 2023

7 CONCLUSÃO

Este trabalho buscou responder a seguinte questão de pesquisa: **- Quais as funcionalidades do software de segurança Endian *Firewall Community*?**

O objetivo geral deste trabalho foi o de identificar e descrever as funcionalidades do *firewall Endian*, usados em redes de computadores.

O estudo permitiu identificar as funcionalidades mais usadas no *Endian Firewall* são: *OpenVPN*, *Proxy* e *Firewall*. Não foram exploradas todas as funções, apenas aquelas que foram julgadas mais essenciais no dia a dia, seja de empresas ou redes domésticas.

Em todos os testes, a configuração foi confirmada, sendo possível validar:

- O *Proxy*, para filtrar e barrar informações.
- O VPN, para criar um túnel, criando um acesso direto ao servidor e
- O *firewall*, criando uma regra de validação, permitindo apenas que determinado cliente pudesse se conectar.

O processo de instalação do Endian *Firewall* em uma máquina virtual foi detalhadamente abordado, desde o download da imagem do software até a configuração das portas de rede. A criação das interfaces verde e vermelha, juntamente com as configurações de rede interna, proporcionou um ambiente seguro e controlado para o *firewall* operar.

A instalação do *Endian Firewall* foi guiada passo a passo, desde a tela inicial após o boot do sistema até a conclusão, destacando a configuração da interface web e suas opções. A seção sobre as funções do *Endian Firewall* explorou aspectos importantes, como o servidor *OpenVPN*, o *firewall* e o *proxy*, visando oferecer uma compreensão abrangente das capacidades do *software*.

O estudo permitiu concluir que os experimentos realizados, como a instalação do *Kali Linux*, a configuração do *Proxy* para bloquear sites específicos e a implementação do *OpenVPN*, proporcionaram uma aplicação prática das funcionalidades do *Endian Firewall*, comprovando sua eficacia. A configuração do *firewall* para permitir o tráfego desejado e a criação de regras específicas, como o redirecionamento de portas para a área de trabalho remota, demonstrou a flexibilidade e adaptabilidade do sistema às necessidades do administrador de rede.

Observou-se também que a instalação e configuração bem-sucedidas do *Endian Firewall*, aliadas aos experimentos realizados, destacaram a eficácia e a versatilidade desta ferramenta como uma solução de segurança robusta para ambientes de rede. A compreensão das diversas funcionalidades oferecidas pelo *Endian Firewall* possibilita seu uso em ambientes empresariais e residenciais, proporcionando controle e proteção eficazes contra ameaças de segurança.

Para continuidade desta pesquisa sugere-se o seguinte trabalho futuro:

- pesquisar e especificar o IPCOP (esse é o sistema que o *Endian* foi criado) e customizar o próprio sistema baseado no mesmo.

8 REFERÊNCIAS

AO KASPERSKY LAB. **Como configurar uma rede doméstica segura**. [S. l.], 2023. Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/how-to-set-up-a-secure-home-network>. Acesso em: 23 mar. 2023.

ABNT. ABNT NBR ISO/IEC 27002. *In*: **Tecnologias da informação - Técnincas de Segurança**. Profjefer.files.wordpress.com, 8 ago. 2005. Disponível em: <https://profjefer.files.wordpress.com/2013/10/nbr_iso_27002-para-impressc3a3o.pdf>. Acesso em: 19 mar. 2023.

BRANDÃO, Guilherme Henrique Freitas. Segurança da informação nas redes sociais: um estudo teórico e experimental sobre as redes sociais. **Riscos**, PUC Goiás, 6 dez. 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/2775>. Acesso em: 19 mar. 2023.

COOPERATI *et al*. **Conhecendo o Endian Firewall**. [*S. l.*]: Vagner Fonseca, 2017. Disponível em: <https://cooperati.com.br/2014/09/conhecendo-o-endian-firewall/>. Acesso em: 2 abr. 2023.

COMO INSTALAR o Kali Linux. [*S. l.*], 30 nov. 2022. Disponível em: https://www.linuxadictos.com/pt/como-instalar-kali-linux.html. Acesso em: 10 set. 2023.

CONCEIÇÃO, RAQUEL MARINA *et al*. SISTEMA FIREWALL PARA O AMBIENTE ACADÊMICO DO INSTITUTO DE CIÊNCIAS EXATAS E APLICADAS. **ICEA UTILIZANDO O PROTOCOLO OPENFLOW**, [*S. l.*], p. 16-69, 1 jan. 2018. Disponível em: <https://www.monografias.ufop.br/bitstream/35400000/1231/16/MONOGRAFIA_SistemasFirewallAmbiente.pdf>. Acesso em: 23 abr. 2023.

CISCO SYSTEMS, INC. O que é um firewall?. *In*: **O que é um firewall?**. [*S. l.*], 2023. Disponível em: https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html#~related-topics. Acesso em: 12 dez. 2023.

DOURADO, Rafael dos Santos. Um Estudo dos Softwares Endian Firewall e PFSense Firewall. **Segurança da informação**, pucgoias, 9 dez. 2022. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/5069>. Acesso em: 19 mar. 2023.

E-TINET *et al*. **Endian Firewall: Como Instalar Uma Solução Completa De Firewall?**. [*S. l.*]: Pedro Delfino, 2023. Disponível em: <https://e-tinet.com/endian-firewall-instalar/>. Acesso em: 2 abr. 2023.

ENDIAN *et al*. **Endian Firewall Community**. [*S. l.*], 2023. Disponível em: <https://www.endian.com/community/features/>. Acesso em: 9 abr. 2023.

ENDIAN. **4i Edge X 6.5 Reference Manual**. [*S. l.*], 18 maio 2023. Disponível em: <http://docs.endian.com/6.5/4i/>. Acesso em: 15 abr. 2023.

FIA BUSSINES SCHOOL. Segurança da informação: o que é, 5 pilares e como garantir nas empresas?. **Segurança da informação**, fia.com.br, 16 dez. 2022. Disponível em: <https://fia.com.br/blog/seguranca-da-informacao/>. Acesso em: 19 mar. 2023.

FIREWALL definição : Aprimore seus conhecimentos sobre segurança. [*S. l.*], 2020. Disponível em: https://ostec.blog/seguranca-perimetro/firewall-definicao/. Acesso em: 13 dez. 2023.

GOV.BR. **90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa: Segundo a Pesquisa Nacional por Amostra de Domicílios, isso significa 65,6 milhões de domicílios conectados, portanto, 5,8 milhões a mais do que em 2019**. [S. l.], 2022. Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa>. Acesso em: 25 mar. 2023.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa.** 6. ed. São Paulo: Editora Atlas Ltda., 2017.

IRKO *et al*. **Cybersecurity: quais são as principais normas e qual sua relação com a LGPD?**. [S. l.]: IRKO, 2021. Disponível em: <https://site.irko.com.br/blog/cybersecurity/>. Acesso em: 26 mar. 2023.

IBICT. Ciência da Informação. **Segurança da informação**, revista.ibict, 2 jan. 2022. Disponível em: <https://revista.ibict.br/ciinf/issue/view/318/90>. Acesso em: 19 mar. 2023.

KALI. **Import Pre-Made Kali VirtualBox VM**. [*S. l.*], 22 ago. 2022. Disponível em: https://www.kali.org/docs/virtualization/import-premade-virtualbox/. Acesso em: 16 set. 2023.

KAKIHATA, Eduardo Massato; SAPIA, Helton Molina; OIKAWA, Ronaldo Toshiaki; PEREIRA, Danillo Roberto; SILVA, Francisco Assis. **SEGURANÇA EM REDES DE COMPUTADORES USANDO SISTEMAS DE DETECÇÃO DE INTRUSÃO BASEADOS EM FLUXOS**. Unoeste, 10 mar. 2016. Disponível em: <https://journal.unoeste.br/index.php/ce/article/view/1446>. Acesso em: 19 mar. 2023.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 8º. ed. [*S. l.*]: Editora Atlas S.A., 2017. 375 p.

MACHADO, Cézar Henrique Junio Pontes. **RANSOMWARE: SEGURANÇA DA INFORMAÇÃO E PREVENÇÃO**. 2021. Monografia (Conclusão do curso) - Pontifícia Universidade Católica de Goiás, Escola de Ciências Exatas e da Computação, Goiânia.

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.

MOLINA, Denilson; SILVEIRA, Sidnei Renato, SANTOS, Fernando Beux; **Um estudo de Caso sobre a Implantação de um Ambiente de Segurança de Redes de Computadores**. Revistas.unifacs.br, 1 jun. 2019. Disponível em: <https://revistas.unifacs.br/index.php/rsc/article/view/5904/3808>. Acesso em: 19 mar. 2023.

NIICONSULTING. **ISO 27004 – Information Security Metrics Implementation. [S. l.]: Akshay Sudan, 2013**. Disponível em: <https://niiconsulting.com/checkmate/2013/07/iso-27004-information-security-metrics-implementation/>. Acesso em: 25 mar. 2023.

PUCPR. **ISO 27000: tudo o que você precisa saber para se destacar na segurança da informação**. [S. l.]: Olívia Baldissera, 2021. Disponível em: <https://posdigital.pucpr.br/blog/iso-27000>. Acesso em: 25 mar. 2023.

PROMOVESOLUCOES. **ISO 27002: O que é e qual sua importância para a LGPD?**. [S. l.]: Rafael Rodrigues, 2021. Disponível em: <https://promovesolucoes.com/iso-27002-o-que-e-e-qual-sua-importancia-para-a-lgpd/>. Acesso em: 26 mar. 2023.

PTCOMPUTADOR *et al*. **Requisitos de hardware Firewall Endian**. [*S. l.*], 2022. Disponível em: <http://ptcomputador.com/Networking/network-security/76497.html>. Acesso em: 2 abr. 2023.

QUALIDADEONLINE *et al*. **Dá para medir a eficácia da segurança da informação em sua empresa?.** [S. l.]: Hayrton, 2017. Disponível em: <https://qualidadeonline.wordpress.com/tag/seguranca-da-informacao/>. Acesso em: 2 abr. 2023.

SILVA, Dione Gelton. **Segurança da informação por meio de redes neurais artificiais**. [*S. l.*], 10 out. 2021. Disponível em: <https://www.nucleodoconhecimento.com.br/tecnologia/artificiais>. Acesso em: 19 mar. 2023.

STATISTA. **Number of internet users worldwide from 2005 to 2022**. [S. l.], 2022. Disponível em: <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/>. Acesso em: 25 mar. 2023.

TECHREPUBLIC *et al*. **SolutionBase: Use the Web interface to configure and monitor an IPCop firewall**. [*S. l.*]: Jason Hiner, 2004. Disponível em: <https://www.techrepublic.com/article/solutionbase-use-the-web-interface-to-configure-and-monitor-an-ipcop-firewall/>. Acesso em: 2 abr. 2023.

VIVAOLINUX *et al*. **O que é o IPCop Firewall**. [*S. l.*]: Alan Cota, 2005. Disponível em: <https://www.vivaolinux.com.br/artigo/IPCop-Firewall-Uma-otima-opcao-de-protecao-para-sua-rede-ADSL/>. Acesso em: 2 abr. 2023.

WLTECH *et al*. **Tipos de conexão de rede no VirtualBox**. [*S. l.*]: Leonardo Garcia, 2019. Disponível em: <https://wltech.com.br/tipos-de-conexao-de-rede-no-virtualbox/#page-content>. Acesso em: 16 abr. 2023.

WAZLAWICK, Raul Sidnei. **Metodologia de Pesquisa Para Ciência da Computação**. [*S. l.*]: Elsevier Editora Ltda., 2014,.

WIKIPEDIA. Segurança da informação. *In*: **Segurança da informação**. [*S. l.*], março 2019. Disponível em: https://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o#. Acesso em: 12 dez. 2023.

APÊNDICE A – TERMO DE AUTORIZAÇÃO DE PUBLICAÇÃO DE PRODUÇÃO ACADÊMICA

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR
Av. Universitária, 1069 • Setor Universitário
Caixa Postal 86 • CEP 74605-010
Goiânia • Goiás • Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br • reitoria@pucgoias.edu.br

RESOLUÇÃO nº 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O estudante José Rodrigo da Fonseca Gomes do Curso de Ciência da Computação, matrícula 20171002801021, telefone: 62 981252559 e-mail fonseca94@live.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado SEGURANÇA DE REDES DE COMPUTADORES: UM ESTUDO SOBRE O ENDIAN FIREWALL, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 14 de Dezembro de 2023.

Assinatura do autor: gov.br Documento assinado digitalmente JOSE RODRIGO DA FONSECA GOMES Data: 14/12/2023 22:16:32-0300 Verifique em https://validar.iti.gov.br

Nome completo do autor: JOSÉ RODRIGO DA FONSECA GOMES

Assinatura do professor–orientador: SOLANGE DA SILVA

Nome completo do professor-orientador: gov.br Documento assinado digitalmente SOLANGE DA SILVA Data: 16/12/2023 19:45:03-0300 Verifique em https://validar.iti.gov.br