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

ESTUDO DE REGRAS DE FIREWALL PARA AMBIENTES DE PEQUENO PORTE

FABIO APARECIDO LOIOLA SILVA JUNIOR

GOIÂNIA
2024

FABIO APARECIDO LOIOLA SILVA JUNIOR

ESTUDO DE REGRAS DE FIREWALL PARA AMBIENTES DE PEQUENO PORTE

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

Orientador (a): Prof. M.E.E. Marcelo Antonio Adad de Araújo.

GOIÂNIA
2024

FABIO APARECIDO LOIOLA SILVA JUNIOR

ESTUDO DE REGRAS DE FIREWALL PARA AMBIENTES DE PEQUENO PORTE

Este trabalho de Conclusão de Curso julgado adequado para obtenção o título de Bacharel em Engenharia de Computação, e aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, em /12/2024.

Prof. Dr. Luiz Álvaro de Oliveira Junior
Coordenador de Trabalho de Conclusão de Curso

Banca examinadora:

Orientador: Prof. Marcelo Antonio Adad de Araújo, M.E.E.

Prof. Carlos Alexandre Ferreira de Lima, M.E.E.

Prof. Nilson Cardoso Amaral, PhD.

GOIÂNIA
2024

Com alegria e gratidão, dedico este trabalho à minha família e amigos, que sempre acreditaram nos meus sonhos e na minha capacidade, sendo fonte constante de apoio e inspiração. Também aos colegas de curso, com quem compartilhei momentos inesquecíveis e criei histórias que levarei para a vida inteira.

RESUMO

Este trabalho apresenta um estudo sobre as regras e normas de *firewall* empregando um Raspberry Pi 4 como base de hardware, visando explorar suas capacidades e avaliar sua eficácia como solução de segurança em redes de pequeno porte. *Firewall* são soluções de segurança de rede onde servem como filtro para melhor proteção de um ambiente de pequeno porte, atendendo a limitações de sites ou sistemas exigidos, podendo evitar acessos de sites indevidos ou mesmo fora do ramo de trabalho utilizado. Para a configuração de *firewall* é necessário entender sobre suas regras e sobre as necessidades do ambiente atuado, podendo ter um melhor desempenho e evitando possíveis ataques. Neste trabalho é realizado um estudo sobre as principais formas de aplicar regras, explicando maneiras de evitar erros na hora de implementar. Regras de filtros de *firewalls* tem de ser escritas cuidadosamente e organizadas de forma a implementar corretamente a política de segurança. Inserir ou modificar uma regra de filtragem requer a devida análise da relação entre uma regra e outras, de forma a determinar a ordem correta entre elas e submetê-la a *updates*.

Palavras-chave: Regras. *Firewall*. Política de Segurança. Ataques. Raspberry Pi.

ABSTRACT

This paper presents a study on firewall rules and standards using a Raspberry Pi 4 as a base, aiming to explore its capabilities and assess its effectiveness as a security solution in small networks. Firewalls are network security solutions that serve as filters to better protect the environment. They address limitations of required sites or systems, potentially preventing users from accessing inappropriate sites or sites outside the relevant field of work. For firewall configuration, it is essential to understand its rules and the specific needs of the environment in order to achieve better performance and prevent potential attacks. This paper studies the main ways to apply rules, explaining methods to avoid mistakes during implementation. Firewall filtering rules must be carefully written and organized to correctly implement the security policy. Adding or modifying a filtering rule requires proper analysis of the relationship between one rule and others to determine the correct order among them and submit it to updates.

Keywords: Rules. Firewall. Security Policy. Attacks. Raspberry Pi.

LISTA DE TABELAS

Tabela 1 - Comparação Modelos OSI e TCP/IP.....26
Tabela 2 – Estrutura Iptables.....39

LISTA DE ABREVIATURAS

Prof.	Professor
M.E.E.	Mestre em Engenharia Elétrica
PhD.	*Philosophiae Doctor* (Doutor em Filosofia)

LISTA DE SIGLAS

HTTP	*Hypertext Transfer Protocol* (Protocolo de Transferência de Hipertexto)
HTTPS	*Hypertext Transfer Protocol Secure* (Protocolo de Transferência de Hipertexto Seguro)
IoT	*Internet of Things* (Internet das Coisas)
IP	*Internet Protocol* (Protocolo de Internet)
ISO	*International Organization for Standardization* (Organização Internacional de Normalização)
LAN	*Local Area Network* (Rede Local)
OSI	*Open Systems Interconnection* (Interconexão de Sistemas Abertos)
SBC	*Single Board Computer* (Computador de Placa Única)
SEO	*Search Engine Optimization* (Otimização de Mecanismos de Busca)
SGSI	Sistema de Gestão de Segurança da Informação
SSL	*Secure Socket Layer* (Camada de Soquete Seguro)
TLS	*Transport Layer Security* (Segurança da Camada de Transporte)
UDP	*User Datagram Protocol* (Protocolo de Datagrama do Usuário)
URL	*Uniform Resource Locator* (Localizador Uniforme de Recursos)
WAN	*Wide Area Network* (Rede de Área Ampla)
WI-FI	*Wireless Fidelity* (Fidelidade sem fios)
WWW	*World Wide Web* (Rede de Alcance Mundial)

LISTA DE FIGURAS

Figura 1 – Firewall.....12
Figura 2 – Intranet / Extranet / Intranet.....29
Figura 3 – Placa Raspberry Pi 4.....33
Figura 4 – Interface inicial de instalação SO.....34
Figura 5 – Escolha da placa.....35
Figura 6 – Versão Raspberry Pi OS.....35
Figura 7 – Loading de Instalação.....36
Figura 8 – Update e Upgrade do sistema.....41
Figura 9 – Instalação do pacote iptables.....42
Figura 10 – Remoção de regras.....11
Figura 11 – Instalação do pacote DHCP.....44
Figura 12 – Atualização e acesso ao painel DHCP.....44
Figura 13 – Configuração do IP Estático.....45
Figura 14 – Regras de política padrão.....46
Figura 15 – Definição de tráfego local.....47
Figura 16 – Permissão SSH / HTTP / HTTPS.....48
Figura 17 – Bloqueio IP estático.....48
Figura 18 – Registro de Log.....50
Figura 19 – Instalação do pacote Persistent.....50
Figura 20 – Aviso de Salvamento Automático.....51
Figura 21 – Teste DHCP junto ao roteador internet.....52
Figura 22 – Teste de conexão ao IP do Google.....53
Figura 23 – Instalação pacote servidor Web.....54
Figura 24 – Teste localhost junto ao servidor Web apache.....55
Figura 25 – Conexão remota com outro dispositivo.....56
Figura 26 – Ping ao IP da Raspberry via dispositivo remoto.....56
Figura 27 – Escaneamento de portas com Nmap.....57
Figura 28 – Teste remoto de conexão a placa negado.....58
Figura 29 – Instalação do pacote de registro de Log’s.....59
Figure 30 – Registro de Log’s.....59

SUMÁRIO

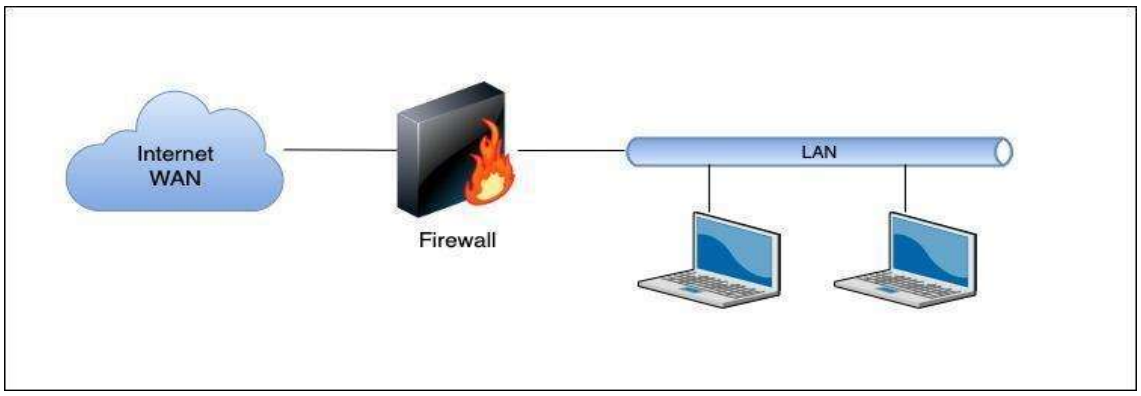
1 Introdução 12
1.1 Objetivos 13
1.1.1 Objetivo geral 13
1.1.2 Objetivos específicos 13
1.2 Justificativa 14
1.3 Procedimentos metodológicos 15
2 Fundamentação Teórica – Redes de Computadores 17
2.1 Segurança de Redes 17
2.2 A necessidade de segurança de redes em um ambiente 18
2.3 Redes de computadores 19
2.4 Técnicas para defesa de redes 20
2.4.1 Política de segurança 20
2.4.2 Firewall 20
2.4.3 Pilares para segurança de redes 21
2.5 Internet das coisas 23
2.6 Modelo OSI 24
2.7 TCP/IP 25
2.8 Os três mundos da conectividade 26
2.8.1 Internet 26
2.8.2 Extranet 27
2.8.3 Intranet 27
2.9 WWW 28
2.10 HTTP 29
2.11 HTTPS 30
3 Configuração da Single Board Computes 32
3.1 Raspberry Pi 32
3.2 Raspberry Pi OS 33
3.2.1 Instalação do Sistema Operacional 34
3.2.2 Vantagens do Raspberri Pi OS 36
3.3 Iptables 37
3.3.1 Estrutura do Iptables 37
3.3.1.1 Tables 37
3.3.1.2 Chains 38
3.3.1.3 Targets 38
3.3.2 Principais aplicações 39
3.3.2.1 Firewall 39
3.3.2.2 Roteamento e Nat 39
3.3.2.3 Rate Limiting 39
3.3.2.4 Monitoramento de Tráfego 40
4 Implementação de Regras 41
5 Análise de Resultados 52
6 Considerações finais 60
6.1 Trabalhos futuros 62

1 Introdução

A segurança de rede é uma área focada na proteção de redes de computadores contra ameaças virtuais. Seus principais propósitos incluem a prevenção do acesso não autorizado aos recursos de rede, a detecção e interrupção de ataques cibernéticos, bem como as violações de segurança, e assegurar que os usuários autorizados desfrutem de acesso seguro aos recursos de rede necessários. Para a segurança, um dos principais métodos é a implementação de um *firewall* na rede, possibilitando proteger e filtrar recursos da organização.

Firewall é uma tecnologia de segurança de rede, responsável por supervisionar e regular o tráfego de dados que atravessa uma rede. Ao filtrar os pacotes de dados que entram e saem da rede, o *firewall* é capaz de identificar e neutralizar ameaças, como *malware* e ataques de negação de serviço. Além disso, ele facilita a criação de políticas de acesso para limitar o tráfego não autorizado ou indesejado. Os *firewalls* se apresentam em diversos tipos, desde os implementados em software, como aqueles integrados a sistemas operacionais, até os baseados em hardware, que consistem em dispositivos especializados para essa finalidade. (Tanenbaum, 2011). A figura 1 ilustra posicionamento do firewall entre rede externa e rede interna, sendo o mais comum e tradicional.

Figura 1 - Firewall



Fonte: De autoria própria.

A seleção da plataforma para implementar um *firewall* é um elemento crítico na garantia da segurança da rede. Optar por utilizar um *Single Board Computer* (SBC), como o Raspberry Pi, para essa finalidade oferece uma série de vantagens significativas. Além de ser uma solução de baixo custo e consumo de energia, a implementação de um *firewall* em um Raspberry Pi proporciona flexibilidade excepcional na configuração e personalização do sistema de proteção da rede. (Kurose, James F, 2013)

A importância de configurar corretamente o *firewall* é garantir a segurança eficaz da rede. Este estudo investigará os benefícios e desvantagens da escolha de um Raspberry Pi como plataforma de *firewall,* implementando regras e considerações essenciais para assegurar a segurança da rede.

O presente trabalho, é uma continuação de um Trabalho de Conclusão de Curso, apresentado pelo acadêmico Hebert Cordeiro de Souza na PUC-GO. Além da implementação de um firewall em uma Raspberry Pi 4, as principais diferenças exploradas são o sistema operacional utilizado e o foco na implementação de regras para segurança. Neste sentido, os dois trabalhos se completam.

1.1 Objetivos

Esta seção visa apresentar e descrever os objetivos gerais e específicos deste trabalho

1.1.1 Objetivo Geral

O objetivo geral deste trabalho é realizar um estudo referente à segurança de redes de computadores, levando em conta normas e possíveis regras que auxiliam e são efetivas para a segurança de rede em um ambiente de pequeno porte.

1.1.2 Objetivos Específicos

Os objetivos específicos deste trabalho são:

- Obter conhecimento mais aprofundado na área de segurança de redes, voltado a um equipamento específico.
- Desenvolver um estudo referente a regras de *firewall* e como implementá-las evitando conflitos entre si, além de possíveis erros.
- Examinar os principais obstáculos e ameaças à segurança que ambientes de pequeno porte enfrentam e como firewall usando Raspberry Pi pode ajudar a reduzir esses perigos.
- Analisar o uso de Raspberry Pi como base para *firewall* em comparação com outras opções de segurança de rede, considerando custos e benefícios.

1.2 Justificativa

A relevância desse estudo se dá pelo aumento da utilização de *Single Board Computer* (Computador de Placa Unica) em projetos de Internet das Coisas (IoT) e, consequentemente, pela crescente necessidade de segurança desses dispositivos.

Com o crescente número de dispositivos conectados à internet, a segurança se torna uma questão crítica. A falta de proteção pode resultar em perda de dados e danos financeiros significativos para as empresas. A criação e implementação de regras de *firewall* em um SBC, além de garantir a segurança do dispositivo, também pode aumentar a proteção dos dados trafegados na rede.

Além disso, a utilização de um Raspberry Pi como plataforma para desenvolvimento de *firewall* pode ser uma alternativa mais econômica e acessível para pequenas e médias empresas que desejam aumentar a segurança de suas redes. Dessa forma, o estudo pode contribuir para disseminar a importância da segurança em projetos de IoT e ajudar na difusão de soluções de segurança mais acessíveis e eficientes para empresas de menor porte.

Este trabalho desenvolve um conjunto de regras de *firewall* eficazes, específicas para ambientes de pequeno porte, que possam ser implementadas em um Raspberry Pi. Através de testes e validações, é possível avaliar a eficiência dessas regras na proteção contra diversas ameaças cibernéticas. O objetivo final é oferecer uma solução prática e econômica que aumente a segurança das redes de pequenas

e médias empresas, promovendo a conscientização sobre a importância da segurança digital em todos os níveis empresariais.

1.3 Procedimentos metodológicos

O presente estudo tem como objetivo desenvolver e avaliar regras de *firewall* eficazes para ambientes de pequeno porte, utilizando um Raspberry Pi 4 como plataforma experimental. A metodologia adotada combina pesquisa bibliográfica e pesquisa experimental.

Quanto aos procedimentos técnicos, esta pesquisa é bibliográfica e experimental. Definir a pesquisa bibliográfica e a pesquisa experimental.

Conforme Gil (2017), a pesquisa bibliográfica segue um conjunto de etapas essenciais para sua efetividade:

a) Escolha do Tema: Estudo de Regras de *Firewall* para Ambientes de Pequeno Porte.

b) Levantamento Bibliográfico Preliminar: A etapa seguinte envolve um mergulho inicial no tema, buscando familiarização e aprofundamento. Através de pesquisas em bases de dados especializadas como Capes e Google Scholar, além de livros relevantes do acervo pessoal, o pesquisador obtém uma visão geral do tema e identifica pontos de pesquisa promissores.

c) Formulação do Problema: Como desenvolver e avaliar regras de *firewall* eficazes para ambientes de pequeno porte utilizando um Raspberry Pi 4?

d) Busca das Fontes: Foram buscados artigos científicos em plataformas tais como Capes, livros e materiais relevantes que compõem o arsenal de informações que sustentarão o estudo. Além de TCCs nos repositórios das universidades.

e) Leitura do Material: Foram realizadas leituras atentas e críticas do material selecionado para identificar os pontos chave relacionados ao tema de pesquisa.

f) Fichamento: Para organizar as informações coletadas, a elaboração de fichas de citação se torna essencial. Cada ficha registra as citações importantes do material bibliográfico, permitindo um acesso rápido e organizado às informações durante a pesquisa.

De acordo com Wazlawick (2014), a pesquisa experimental consiste na análise de dados coletados por meio de experimentos sistematizados. Isso inclui a implementação prática das regras de *firewall* e a avaliação de sua eficácia.

a) Configuração do Ambiente: Configurar um Raspberry Pi 4 como *firewall*. O dispositivo será conectado entre um roteador e os dispositivos da rede interna.

b) Implementação das Regras: Implementar diferentes conjuntos de regras de *firewall* utilizando *iptables*. As regras serão desenvolvidas com base nas melhores práticas identificadas na pesquisa bibliográfica.

c) Teste e Avaliação: Realizar testes de penetração e monitoramento de tráfego para avaliar a eficácia das regras. Serão utilizadas ferramentas como *Wireshark* para análise de tráfego.

d) Análise dos Dados: Análise quantitativa dos resultados dos testes de penetração e monitoramento de tráfego. Serão analisados indicadores como número de tentativas de invasão bloqueadas, performance do *firewall* e impacto nas atividades da rede.

Para realizar a implementação do Raspberry Pi como plataforma de *firewall*, são realizados os seguintes procedimentos metodológicos:

- Revisão bibliográfica: Será conduzida uma pesquisa sobre as principais soluções de firewall disponíveis, incluindo o uso do Raspberry Pi, com o objetivo de avaliar suas vantagens, desvantagens e identificar as melhores práticas para configuração e segurança.
- Seleção de equipamentos: Serão escolhidos os componentes necessários para o projeto, como Raspberry Pi 4, cartão SD, cabo de energia, cabo Ethernet, além de periféricos como mouse, teclado e monitor.
- Instalação do sistema operacional: Será efetuado o download e a instalação do sistema operacional Raspberry Pi OS, configurando-o para atender às necessidades do projeto.
- Análise dos resultados: Os resultados obtidos durante os testes e avaliações serão examinados, comparando a eficiência de regras implementadas.

2 Fundamentação Teórica – Redes de Computadores

Este capítulo apresenta o Referencial Teórico indispensável para a elaboração deste trabalho, reunindo conceitos e definições fundamentais para a compreensão do projeto. Além disso, inclui pesquisas bibliográficas relevantes que embasam e contextualizam o tema abordado neste trabalho de conclusão de curso.

2.1 Segurança de Redes

A cibersegurança, ou segurança de computadores, concentra-se na proteção de *softwares*, *hardwares* e redes para prevenir ataques cibernéticos aos sistemas da empresa. Seu objetivo é garantir que as informações digitais sejam gerenciadas, transmitidas e armazenadas de forma segura. Isso envolve medidas como a instalação de antivírus, *firewalls,* a realização de *backups* dos dados dos servidores, a criptografia de informações e a implementação de tecnologias de assinatura digital. Essas ações dificultam a perda permanente de informações e ajudam a evitar possíveis fraudes.

A cibersegurança, teve sua origem na computação com um foco inicial na segurança física dos primeiros computadores. Com a expansão das redes de computadores, especialmente com o surgimento da internet, as preocupações se voltaram para a proteção das comunicações entre sistemas. Ao longo das décadas seguintes, o crescimento exponencial da conectividade e o aumento dos ataques cibernéticos impulsionaram o desenvolvimento de medidas de segurança mais sofisticadas.

Nos anos mais recentes, a cibersegurança tornou-se uma prioridade crítica para empresas e governos, com o surgimento de regulamentações mais rigorosas e a adoção de tecnologias avançadas, para fortalecer as defesas cibernéticas.

A ABNT NBR ISO/IEC 27001:2013 é uma norma brasileira que adota a ISO/IEC 27001:2013 internacionalmente reconhecida. Essa norma estabelece os requisitos para um sistema de gestão de segurança da informação (SGSI), proporcionando uma abordagem abrangente para a gestão da segurança da informação em uma organização. Ela define os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação, levando

em consideração os contextos interno e externo da organização, bem como os requisitos legais e regulamentares relevantes.

Conforme a ABNT NBR ISO/IEC 27001:2013, a segurança da informação é assegurada pela preservação da confidencialidade, integridade e disponibilidade dos dados. Isso é alcançado por meio da implementação de uma variedade de controles, que abrangem processos, tecnologias e práticas de gestão de riscos.

Por outro lado, segundo a ABNT NBR ISO/IEC 27032:2012, a cibersegurança engloba a proteção não apenas dos dados, mas também da privacidade, propriedade intelectual, ativos financeiros e informações pessoais. Ela visa prevenir não só o acesso não autorizado, como a interrupção das operações comerciais e os impactos associados ao uso, armazenamento e transmissão de dados por meio de redes de computadores ou outros meios eletrônicos.

2.2 A necessidade de segurança de redes em um ambiente

De acordo com Nakamura e Geus (2007), a segurança de redes é necessária e deve ser bem definida, levando em conta custos e benefícios, pois não existe uma segurança invulnerável. A segurança de redes é uma área crucial no mundo digital.

Em uma era em que a comunicação e o armazenamento de dados são predominantemente digitais, a segurança de redes torna-se uma prioridade incontestável. Desde informações pessoais até dados financeiros e comerciais, a segurança das redes visa garantir que essas informações estejam protegidas contra acesso não autorizado, roubo ou manipulação.

Além disso, a segurança de redes é essencial para preservar a confidencialidade das informações. Muitas vezes, os dados transmitidos pelas redes são de natureza confidencial e privada. Portanto, é crucial que apenas indivíduos autorizados tenham acesso a esses dados, protegendo a privacidade e a segurança das partes envolvidas.

Muitas organizações estão sujeitas a regulamentações que exigem a proteção de dados e informações. A segurança de redes ajuda a garantir o cumprimento dessas regulamentações, protegendo os dados e as informações conforme exigido pelas leis e padrões aplicáveis.

Evitar criar redes sem proteção, pensando que as falhas não serão descobertas, configurar servidores privados na organização para uso doméstico e incluir chaves de criptografia diretamente no código de um software são exemplos de práticas inadequadas que devem ser evitadas. Essa falta de transparência representa um grande risco para a organização, já que, mais cedo ou mais tarde, pode-se descobrir que há uma abertura disponível para ser explorada.

Ainda hoje, existe a ideia de que a segurança é um investimento caro e dispensável, visto como necessário apenas após a ocorrência de um ataque que cause prejuízos à organização. No entanto, apesar dessa mentalidade reativa, algumas empresas estão começando a enxergar a segurança de uma maneira diferente, reconhecendo-a como um componente essencial do negócio.

2.3 Redes de computadores

Segundo Kurose (2013), as redes de computadores são conjuntos de dispositivos eletrônicos conectados entre si, permitindo a troca de informações. Essa comunicação acontece através de uma linguagem comum, como o Protocolo de Internet (IP). Essas redes podem variar em tamanho e estrutura, dependendo de seu propósito. Existem dois tipos principais de redes: públicas e privadas. A Internet é um exemplo de rede pública, conectando milhões de computadores em todo o mundo.

É importante destacar que as redes de computadores podem apresentar vulnerabilidades e riscos de segurança. Por isso, medidas como *firewall*s são necessárias para proteger as informações transmitidas na rede. Em resumo, as redes de computadores são fundamentais para a comunicação entre dispositivos, mas é essencial estar ciente dos riscos de segurança associados a essa troca de informações.

Além disso, as redes de computadores facilitam o compartilhamento de recursos entre dispositivos. Elas podem ser classificadas de acordo com seu tamanho e alcance geográfico, como redes locais (LANs) e redes de longa distância (WANs). Também podem ser classificadas de acordo com sua arquitetura de comunicação, como redes ponto-a-ponto (peer-to-peer) e redes cliente-servidor. (Kurose 2013)

2.4 Técnicas para defesa de redes

2.4.1 Política de segurança

Aborda aspectos como planejamento, elementos essenciais, pontos a serem considerados e desafios comuns enfrentados durante a implementação. Ross (2013) destaca exemplos específicos de áreas que devem ser abordadas pela política de segurança, como políticas de senhas, *firewall* e acesso remoto. Além disso, discute a política de segurança em ambientes cooperativos, que apresentam características próprias.

2.4.2 Firewalls

Firewalls são dispositivos de segurança de rede que monitoram o tráfego de entrada e saída, permitindo ou bloqueando o tráfego específico com base em um conjunto de regras de segurança predeterminadas. Servem como uma barreira entre uma rede confiável e uma rede não confiável, como a internet. Sua função principal é regular e filtrar o tráfego de rede para garantir a segurança e integridade dos dados, seguindo as diretrizes estabelecidas nas regras de segurança.

Evoluiram com o passar dos anos e deixaram de ser somente um filtro de pacotes rudimentar para se tornarem sistemas sofisticados e com capacidade de filtragem cada vez mais avançados. A evolução desse componente de segurança, fornece conceitos técnicos relevantes para a escolha do tipo de *firewall* mais adequado para cada organização, assim como discute as arquiteturas que influenciam o nível de segurança.

Firewalls são itens críticos para a segurança de redes de qualquer tamanho. Eles ajudam a proteger contra ameaças externas, evitar acessos não autorizados e garantir que o tráfego de rede siga políticas de segurança específicas. Sem um *firewall*, redes ficam expostas a uma série de riscos, desde ataques de *malware* até invasões por hackers.

Kurose e Ross (2013) destacam que um firewall funciona filtrando o tráfego de rede com base em regras pré-estabelecidas. O administrador da rede configura essas regras, que determinam quais pacotes de dados são permitidos ou bloqueados. Essas

regras podem depender de critérios como o endereço IP de origem e destino, portas utilizadas, protocolos, entre outros.

Além de controlar o tráfego, os firewalls também podem impor políticas de segurança. Por exemplo, eles podem restringir o acesso a determinados serviços ou sites da Internet, além de bloquear usuários não autorizados. No entanto, como observado por Parker (2023), os firewalls, apesar de essenciais, não oferecem proteção completa contra todas as ameaças. Eles devem ser complementados com outras medidas de segurança, como antivírus, criptografia e sistemas de autenticação de usuários.

Firewall não deve ser considerado como a única medida de defesa para garantir a segurança de uma organização, mas ainda assim é uma das mais usadas e necessárias dentro de um ambiente. (Nakamura, 2007)

2.4.3 Pilares para segurança de redes

Segundo Stallings (2014), há alguns pilares fundamentais em um ambiente para que seja possível eleger segurança para sua rede.

Confidencialidade, se refere à proteção de informações contra acessos não autorizados, garantindo que dados sensíveis sejam acessados apenas por pessoas ou sistemas devidamente autorizados. O principal objetivo da confidencialidade é assegurar que informações privadas ou restritas permaneçam secretas e sejam divulgadas apenas a indivíduos ou entidades autorizadas.

Confidencialidade é responsável pela proteção de dados sensíveis, como dados pessoais, financeiros, médicos e comerciais e, se expostas, podem resultar em danos significativos, incluindo roubo de identidade, fraudes financeiras e violações de privacidade.

Alguns mecanismos utilizados para garantir a confidencialidade são a criptografia que transforma dados em um formato codificado que só pode ser decifrado por aqueles que possuem a chave de decriptação, controles de acesso, que implementa sistemas que garantam que apenas indivíduos autorizados possam acessar determinadas informações, autenticação, verificação da identidade de um usuário e autorização.

As políticas de segurança estabelecem e aplicam padrões que definem como os dados devem ser manipulados, quem tem permissão para acessá-los e sob quais condições. Treinamento e conscientização, que seria educar funcionários e outras partes interessadas sobre a importância da confidencialidade e as melhores práticas para proteger informações sensíveis, monitoramento e auditoria, implementando sistemas para monitorar o acesso e o uso de informações confidenciais e conduzir auditorias regulares para garantir conformidade com políticas de segurança.

Para Stallings (2014) a integridade é outro pilar fundamental da segurança da informação. Ela refere-se à precisão, consistência e confiabilidade dos dados ao longo de seu ciclo de vida. A integridade garante que os dados não sejam alterados de forma não autorizada, acidental ou maliciosamente, e que qualquer modificação seja detectável.

A violação da integridade pode ter graves consequências como dados corrompidos ou alterados levando a decisões equivocadas, afetando negativamente operações e estratégias. Perdas financeira, alterando de forma não autorizada registros financeiros resultando em perdas significativas e fraudes. Tendo também danos na reputação onde a confiança dos clientes e parceiros pode ser abalada se os dados de uma organização forem considerados não confiáveis.

Assim, a integridade é um pilar crucial para garantir que os dados sejam precisos. Implementar medidas eficazes para proteger a integridade dos dados é essencial para a segurança da informação, a continuidade dos negócios e a conformidade regulatória. Proteger a integridade dos dados ajuda a prevenir fraudes, a manter a confiança dos clientes e a garantir operações empresariais eficientes e seguras.

A disponibilidade é o terceiro pilar dado por Stallings (2014), fundamental para segurança da informação, refere-se à capacidade de garantir que informações e recursos estejam acessíveis e utilizáveis por usuários autorizados sempre que necessário. A disponibilidade assegura que os sistemas funcionem de maneira eficiente e que os dados estejam disponíveis no momento e lugar apropriados, sem interrupções indesejadas.

É essencial para garantir que os sistemas e serviços de TI estejam acessíveis e funcionais quando necessários. Implementar medidas robustas para garantir a disponibilidade é fundamental para a continuidade dos negócios, a satisfação do cliente e a conformidade regulatória.

2.5 Internet das coisas (IoT)

De acordo com Kurose (2013) a Internet das Coisas (IoT) é composta por dispositivos e sensores, processadores de baixo custo e conectividade. Os dispositivos e sensores coletam dados do ambiente, como temperatura, umidade e movimento. Os processadores de baixo custo, como microcontroladores, podem também gerenciar esses dados. A conectividade é garantida por redes sem fio como *Wi-Fi* e *Bluetooth*, permitindo a comunicação entre os dispositivos e os sistemas centrais.

O funcionamento da IoT segue três etapas principais: sensoriamento, processamento e atuação. Primeiro, os dispositivos equipados com sensores coletam dados em tempo real do ambiente. Em seguida, esses dados são processados por microcontroladores ou enviados para servidores ou nuvens para processamento adicional. Finalmente, com base nos dados processados, os atuadores executam ações específicas, como ligar ou desligar equipamentos ou ajustar configurações.

A IoT tem uma ampla gama de aplicações em várias áreas. Por exemplo em domicílios, é usada para criar casas inteligentes com controle automatizado de iluminação, temperatura e segurança. Nas indústrias, a IoT facilita o monitoramento e a automação de processos industriais, contribuindo para a Indústria 4.0. Na área da saúde, dispositivos vestíveis monitoram sinais vitais e condições de saúde. Em cidades inteligentes, a IoT é utilizada para a gestão de tráfego, iluminação pública e coleta de lixo eficiente.

Kurose (2013) ressalta que os benefícios da IoT incluem maior eficiência, conveniência e inovação. A IoT melhora a automação e o monitoramento de processos, resultando em operações mais eficientes. Também oferece conveniência ao permitir o controle remoto e a automação de tarefas cotidianas. Além disso, a IoT abre novas possibilidades em diversas áreas, como saúde, transporte e manufatura, impulsionando a inovação.

2.6 Modelo OSI (*Open System Interconnection*)

Um protocolo de rede de computadores pode ser descrito como um conjunto de regras, procedimentos e formatos de mensagens utilizados para a comunicação entre dispositivos conectados a uma rede. Esses protocolos asseguram a transmissão confiável e eficiente de dados, independentemente do tipo de rede ou dos dispositivos envolvidos. Eles são projetados para lidar com diversos aspectos da comunicação, desde o estabelecimento de conexões até a formatação e a entrega de mensagens.

De acordo com Kurose e Ross (2013), os protocolos de rede são organizados em uma arquitetura de camadas, onde cada camada possui funções específicas que, em conjunto, possibilitam a troca de informações entre dispositivos conectados. O modelo OSI (Open Systems Interconnection), desenvolvido pela ISO (*International Organization for Standardization*) na década de 1980, é um exemplo clássico dessa abordagem em camadas. Este modelo é composto por sete camadas, cada uma responsável por diferentes aspectos da comunicação:

- Camada Física: Trata da transmissão de bits puros através do meio físico de comunicação.
- Camada de Enlace: Responsável pela transferência de quadros (*frames*) entre dispositivos em uma mesma rede local.
- Camada de Rede: Gerencia o roteamento de pacotes entre redes distintas.
- Camada de Transporte: Garante a entrega confiável de dados entre sistemas finais.
- Camada de Sessão: Estabelece, gerencia e encerra sessões de comunicação.
- Camada de Apresentação: Converte os dados entre o formato utilizado pela rede e o formato compreensível pelas aplicações.
- Camada de Aplicação: Fornece serviços de rede diretamente às aplicações dos usuários, como e-mail e transferência de arquivos.

Apesar de o modelo OSI não ser implementado diretamente em redes modernas, ele serve como uma referência crucial para o desenvolvimento e padronização de protocolos específicos. Kurose e Ross (2013) pontuam que o modelo

OSI fornece uma estrutura conceitual que facilita a compreensão e o design dos protocolos de rede, ajudando a garantir que diferentes dispositivos possam se comunicar.

2.8 TCP/IP (*Transmission Control Protocol / Internet Protocol*)

A ideia do modelo de referência TCP/IP surgiu durante a Guerra Fria, entre os Estados Unidos e a extinta União Soviética. O Departamento de Defesa Americano tinha como objetivo manter a comunicação entre as bases militares, mesmo que parte delas fosse comprometida em caso de ataques ou catástrofes que afetassem os meios de comunicação. Dessa necessidade, surgiu a ARPANET, uma rede projetada para garantir que, mesmo com a destruição de uma base, a comunicação entre as demais permanecesse intacta.

Para Mendes (2016) quando se menciona TCP/IP, imediatamente se associa à Internet, e o inverso também é verdadeiro: a Internet está diretamente relacionada à arquitetura TCP/IP. Esse modelo possui quatro camadas: a camada de aplicação, a camada de transporte, a camada de Internet e a camada de rede, como mostrado na tabela 1. É importante notar que algumas das camadas do modelo TCP/IP possuem o mesmo nome das camadas no modelo OSI, embora não devam ser confundidas.

- Camada de Aplicação: é a camada mais próxima do usuário final. Ela inclui protocolos que suportam aplicativos de rede, como HTTP para a Web, FTP para transferência de arquivos e SMTP para e-mail.
- Camada de Transporte: responsável por fornecer comunicação de *host* a *host*. Os principais protocolos nesta camada são o TCP (*Transmission Control Protocol*), que garante a entrega confiável dos dados, e o UDP (*User Datagram Protocol*), que permite a transmissão rápida, mas não garantida.
- Camada de Internet: é responsável pela comunicação entre redes. O principal protocolo aqui é o IP (*Internet Protocol*), que define como os pacotes de dados são endereçados e encaminhados para o destino correto.

- Camada de Acesso a Rede: trata da interface com o hardware de rede e a transmissão física dos dados. Inclui protocolos e métodos para transmitir dados sobre um determinado meio físico, seja ele cabos, ondas de rádio ou fibras ópticas.

O modelo TCP/IP, com suas quatro camadas, foi fundamental para o desenvolvimento e expansão da Internet, proporcionando uma estrutura flexível e robusta para a comunicação de dados em redes de computadores.

Tabela 1: Comparação Modelos OSI e TCP/IP

MODELO OSI	MODELO TCP/IP
APLICAÇÃO	APLICAÇÃO
APRESENTAÇÃO	
SESSÃO	
TRANSPORTE	TRANSPORTE
REDE	INTERNET
ENLACE	ACESSO A REDE
FÍSICA	

Fonte: De autoria própria

2.8 Os Três Mundos da Conectividade

2.8.1 Internet

Mesmo aqueles que não são familiarizados com informática precisam entender alguns termos comuns utilizados na internet, pois ao se conectarem, podem se deparar com questões como: o que é WWW, HTTP.

Qualquer usuário com um computador conectado a um modem, pode navegar na rede ao estabelecer uma sessão com o equipamento da operadora provedora de internet. A internet possibilitou o compartilhamento de conhecimento e entretenimento em diversas áreas.

Segundo Mendes (2016) a Internet refere-se à vasta rede global que teve suas origens na ARPANET e evoluiu para se tornar uma confederação de todas as redes TCP/IP interconectadas. Todas essas redes são conectadas por meio de circuitos

digitais de alta velocidade. Além delas existirem redes locais de corporações, conhecidas como Intranets, e redes estendidas para parceiros externos, conhecidas como Extranets.

2.8.2 Extranet

Uma Extranet é uma extensão da Intranet de uma organização que permite a comunicação e colaboração com partes externas, como fornecedores, clientes e parceiros de negócios, através da internet ou de redes geograficamente distribuídas. Ela utiliza enlaces de comunicação privados e os mesmos protocolos do modelo de referência TCP/IP.

Ao contrário da Intranet, que é restrita ao uso interno da organização, a Extranet amplia o alcance dos serviços e recursos para partes externas autorizadas. Isso permite que essas partes acessem informações específicas, como catálogos de produtos, sistemas de pedidos ou colaboração em projetos, enquanto mantêm um nível de segurança e controle sobre o acesso.

Mendes (2016) reforça que as Extranets são voltadas para unidades coorporativas, utilizando com intenção de interligar várias sedes que possuem Intranets independentes, facilitando a comunicação e o compartilhamento de recursos entre diferentes locais. Essa interconexão possibilita uma colaboração eficiente entre os membros de diferentes unidades organizacionais, fornecedores e clientes, melhorando a eficiência e a produtividade nos negócios.

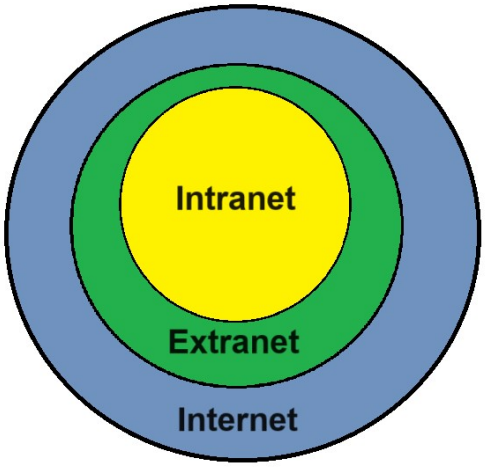
2.8.3 Intranet

Mendes (2016) explica que Intranet é uma rede de propriedade privada que utiliza o modelo de referência TCP/IP e oferece serviços de comunicação semelhantes aos da Internet, mas exclusivamente para uso interno de uma organização. Ela opera com os mesmos protocolos da família TCP/IP e disponibiliza serviços como servidor de páginas Web, servidor DNS, HTTP e servidor de e-mail, entre outros.

Ao contrário da Internet, uma Intranet não está acessível ao público em geral, sendo restrita aos funcionários ou membros autorizados da organização que tenham acesso à rede local interna (LAN), como mostrado no exemplo de profundidade da

figura 2. Isso significa que os serviços e recursos disponíveis na Intranet são acessíveis apenas dentro do ambiente controlado da empresa ou instituição, oferecendo uma plataforma segura para comunicação, colaboração e compartilhamento de informações entre os membros da organização.

Figura 2 – Intranet / Extranet / Internet



Fonte: De autoria própria.

2.9 WWW (*World Wide Web*)

Mendes (2016) cita que o *World Wide Web,* conhecido como WWW, é o principal serviço de internet, sendo a parte multimídia da rede, onde é possível ler jornais eletrônicos, fazer compras em shoppings virtuais, acessar redes sociais e consultar bancos de dados. Além disso, permite que os usuários acessem diversos documentos através de hiperlinks em páginas HTML, crescendo a cada dia e se tornando algo mais comum no dia a dia das pessoas.

Devido à vasta quantidade de informações disponíveis, são necessários serviços de catalogação, agindo como motores de busca, para encontrar informações específicas rapidamente e de maneira eficiente.

A informação na Web é organizada na forma de páginas, que podem conter textos, imagens, sons e vídeos. As páginas são interligadas por meio de hipertextos, formando uma rede de documentos conectados. Isso permite, por exemplo, que um

trabalho acadêmico se refira diretamente a um texto base, facilitando o acesso a fontes e a navegação entre documentos relacionados.

A democratização do acesso à informação, facilitação de comunicação global, oportunidades de comércio eletrônico e suporte a diversas atividades diárias, são considerados benefícios da Web. Ela continua a evoluir, introduzindo novas tecnologias e serviços que aprimoram a forma como se vive e trabalha.

2.10 HTTP (*Hyper Text Transfer Protocol*)

Um dos primeiros elementos que se encontra em uma URL (*Uniform Resource Locator*) é o protocolo HTTP, representado na porção inicial do endereço. Para Mendes (2016) esse protocolo é fundamental, pois estabelece a base para a conexão entre o navegador e o servidor onde o recurso desejado está hospedado. Significa *HyperText Transfer Protocol*, em português Protocolo de Transferência de Hipertexto, é essencialmente a linguagem que o navegador utiliza para se comunicar com o servidor e solicitar a página da Web específica.

O HTTP, é essencial para a comunicação entre o navegador de um usuário e os servidores que hospedam os recursos da World Wide Web (WWW). Criado por Tim Berners-Lee em 1989, o HTTP permite que os usuários acessem e interajam com uma variedade de informações disponíveis na internet.

Na sua essência, o HTTP opera em um modelo cliente-servidor. Aqui, o cliente, geralmente um navegador Web, faz uma solicitação ao servidor para acessar um recurso específico, como uma página da Web, e o servidor responde fornecendo a informação solicitada. Esse processo de troca de informações entre cliente e servidor é fundamental para a funcionalidade do HTTP e possibilita o acesso a uma ampla gama de dados em servidores remotos.

Kurose e Ross (2013) explicam que a estrutura do HTTP é simples, composta por uma linha de requisição, um cabeçalho e, em alguns casos, uma mensagem de corpo. A linha de requisição indica o método utilizado (como GET, POST, PUT, DELETE), o recurso solicitado (URL) e a versão do protocolo. O cabeçalho contém informações adicionais sobre a requisição, como opções de cache e autenticação, enquanto a mensagem de corpo contém os dados enviados pelo cliente, como no caso de uma requisição POST.

Ao longo dos anos, o HTTP passou por diversas versões, cada uma trazendo melhorias em relação à anterior. Desde a sua primeira versão, o HTTP/0.9, até a mais recente, o HTTP/3, lançado em 2020, o protocolo evoluiu para atender às demandas crescentes da Web. Cada versão introduziu novos recursos e aprimoramentos, como a introdução de suporte a cabeçalhos, conexões persistentes e técnicas avançadas de otimização de desempenho, como a multiplexação e a compressão de dados.

Apesar dos avanços, o HTTP ainda enfrenta desafios, especialmente relacionados ao aumento do tráfego na Web. O HTTP é uma peça fundamental da infraestrutura da Web, permitindo que os usuários acessem e interajam com os recursos disponíveis na internet. Sua evolução contínua reflete a constante busca por melhorias e adaptações às necessidades em constante mudança dos usuários e da própria rede.

2.11 HTTPS (Hypertext Transfer Protocol Secure)

O HTTPS (*Hypertext Transfer Protocol Secure*) representa uma evolução do protocolo HTTP, agregando uma camada adicional de segurança à comunicação entre cliente e servidor. Conforme mencionado por Kurose e Ross (2013), o HTTPS utiliza criptografia para salvaguardar os dados em trânsito e garantir a autenticidade do servidor. Inicialmente, o SSL (*Secure Socket Layer*) foi empregado como protocolo de segurança, porém, posteriormente, foi substituído pelo TLS (*Transport Layer Security*) devido à sua maior segurança e eficácia.

De acordo com Forouzan (2006), o HTTPS é uma extensão do HTTP, concebida para proteger a transferência de informações sensíveis pela internet, como senhas e dados financeiros. Sua origem remonta à necessidade de assegurar a privacidade e a integridade dos dados, dada a presença de ameaças na rede.

O funcionamento do HTTPS, conforme explicado por Kurose e Ross (2013), baseia-se no uso de certificados digitais emitidos por autoridades de certificação confiáveis. Estes certificados contêm informações sobre a identidade do proprietário do site. Ao acessar um site com HTTPS, o navegador verifica a validade do certificado e estabelece uma conexão criptografada com o servidor. Todas as informações trocadas entre cliente e servidor são então criptografadas, garantindo que somente o destinatário possa decodificá-las.

O HTTPS desempenha um papel crucial na proteção da privacidade dos usuários, impedindo que dados sensíveis sejam interceptados por terceiros mal-intencionados, conforme afirmado por Tanenbaum e Wetherall (2011). Além disso, o HTTPS ajuda a mitigar ataques de *phishing* e a garantir a autenticidade do site, uma vez que o certificado digital atesta a identidade do proprietário do site. Vale ressaltar também que o HTTPS é um requisito para o SEO (*Search Engine Optimization*), pois os mecanismos de busca privilegiam sites seguros nos resultados de pesquisa.

A importância do HTTPS tem crescido à medida que as pessoas compartilham cada vez mais informações pessoais e financeiras online. Parker (2023) ressalta que o HTTPS é uma das principais medidas de segurança para proteger a privacidade dos usuários e evitar ataques cibernéticos. Portanto, é essencial que desenvolvedores de sites e usuários finais estejam conscientes da importância do HTTPS e saibam como utilizá-lo adequadamente.

3 Configuração da Sigle Board Computer

3.1 Raspberry Pi

O Raspberry Pi é um computador de placa única criado pela *Raspberry Pi Foundation*, projetado para ser uma ferramenta de ensino acessível na área de programação e computação. No entanto, ele rapidamente ganhou popularidade em várias aplicações, incluindo projetos de automação doméstica e soluções de Internet das Coisas em ambientes corporativos.

Sua principal característica é a versatilidade, pois pode ser utilizado em diversas áreas e programado em diferentes linguagens. Sendo uma plataforma ideal para entusiastas e desenvolvedores que desejam criar e experimentar com tecnologias inovadoras. O Raspberry Pi inclui todos os componentes essenciais em uma única placa, como processador, memória, interfaces de rede e portas USB, além de suporte para vídeo e áudio.

Raspberry Pi é capaz de rodar sistemas operacionais completos, como o Linux, e pode ser expandido por meio de acessórios e periféricos, aumentando suas funcionalidades. Um dos atrativos do dispositivo é seu baixo custo e requisitos modestos de hardware, tornando-o uma escolha econômica para vários tipos de projetos.

O Raspberry Pi 4, lançado em 2019, trouxe avanços significativos em desempenho, com um processador ARM Cortex-A72 de 64 bits, até 8 GB de RAM, conectividade Wi-Fi e Bluetooth, além de portas Ethernet, USB e HDMI, sendo uma ferramenta ainda mais robusta para uma amplos projetos.

Atualmente existem versões de Raspberry Pi mais robustas do que a versão 4, porém com um custo mais elevado. É necessário calcular o uso que será feito de tal placa, para entender se será realmente necessário investir em uma versão mais avançada.

Figura 3 – Placa Raspberry Pi 4

Fonte: De autoria própria

3.2 Raspberry Pi OS

O Raspberry Pi OS é o sistema operacional oficial para a família de computadores de placa única Raspberry Pi. Anteriormente chamado de Raspbian, ele é uma distribuição baseada no Debian, otimizada para o hardware do Raspberry Pi. O Raspberry Pi OS é desenvolvido para ser leve e eficiente, adequado para o desempenho limitado desses pequenos computadores, e vem com um conjunto completo de softwares pré-instalados que permitem que o Raspberry Pi seja usado tanto em projetos educacionais quanto em aplicações práticas.

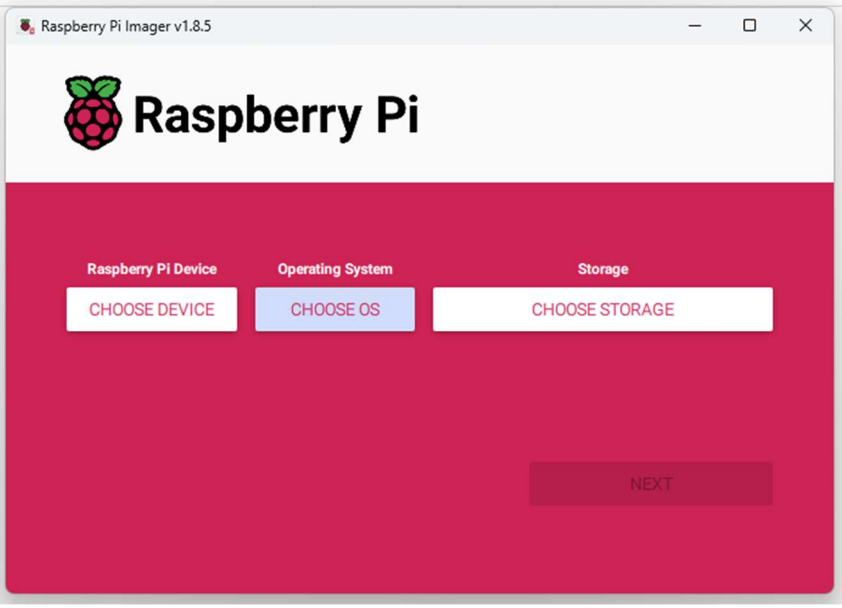
Como é derivado do Debian Linux, o Raspberry Pi OS herda sua estabilidade e uma vasta quantidade de pacotes disponíveis. A comunidade do Debian fornece suporte e atualizações regulares, garantindo que o sistema seja seguro e atualizado. O sistema pode ser usado com uma interface gráfica de usuário, leve e familiar para quem usa desktops tradicionais.

O Raspberry Pi OS vem com uma seleção de softwares que facilitam o aprendizado e o uso em projetos. Além de ser utilizado em escolas e universidades para ensinar programação, eletrônica e conceitos de computação. A leveza do sistema permite que o Raspberry Pi seja usado como um controlador de automação, firewall, servidor de mídia, ou central de IoT.

3.2.1 Instalação do Sistema Operacional

Para a instalação do sistema operacional, é necessário fazer o download do *imager* no próprio site do fabricante. Ao executar o programa de instalação, a interface da tela inicial estará disponível, como mostrado na figura 4.

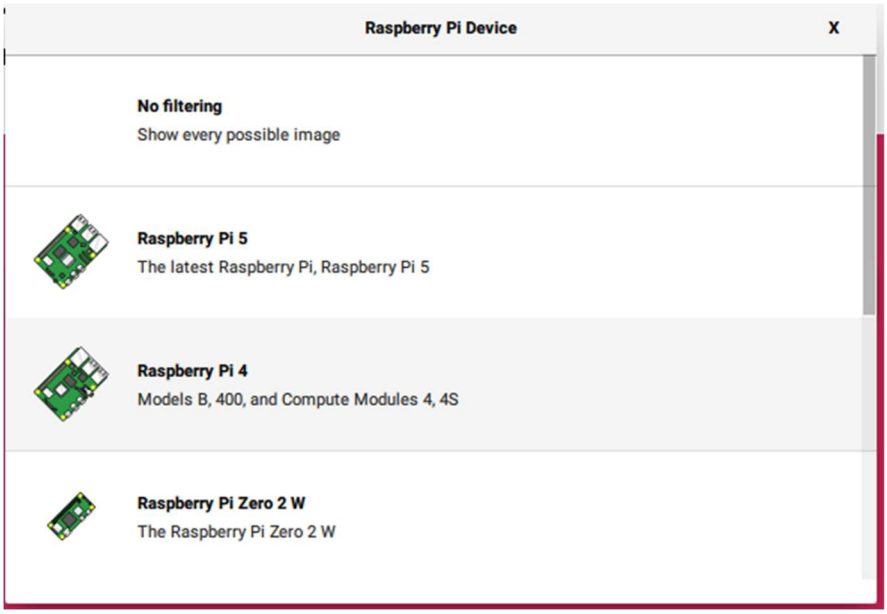
Figura 4: Interface inicial de instalação SO



Fonte: De autoria própria

Com os três campos disponíveis para escolha da preferência, levando em consideração o hardware que será utilizado, escolhe-se dentre as opções o item desejado, como ilustra a figura 5.

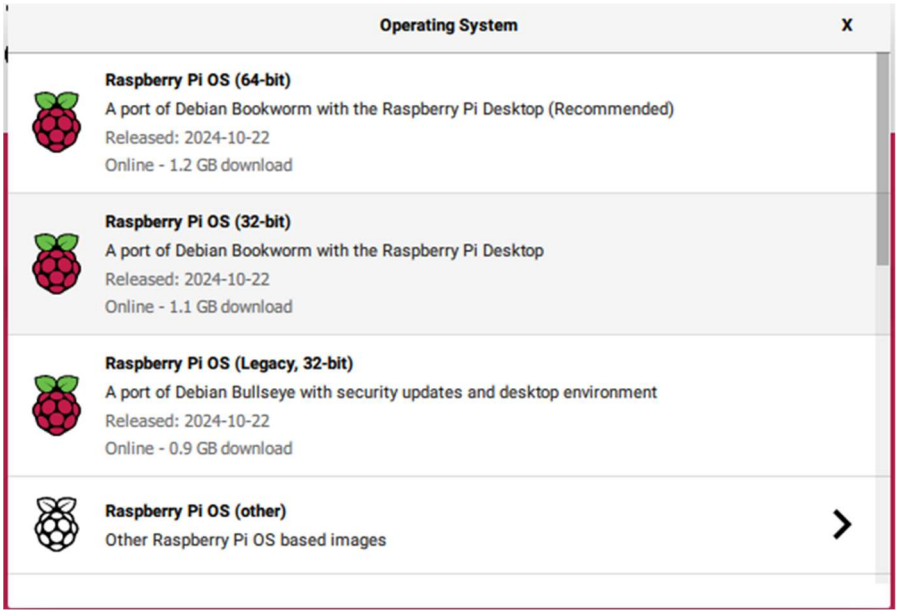
Figura 5: Escolha da placa



Fonte: De autoria própria

Levando ao próximo passo, figura 6, a escolha do sistema operacional desejado, se tratando das variações do próprio Raspberry Pi OS.

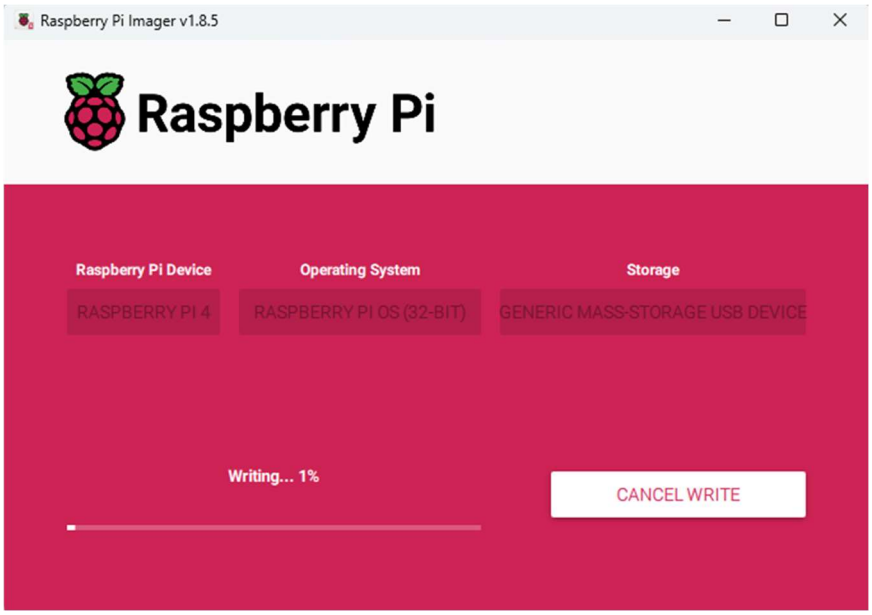
Figura 6: Versão Raspberry Pi OS



Fonte: De autoria própria.

Finalizando as escolhas exigidas para instalação, é necessário informar em qual dispositivo irá gravar o sistema operacional, podendo ser um pendrive ou até mesmo cartão SD, a instalação irá iniciar como mostra a figura 7.

Figura 7: Loading de instalação



Fonte: De autoria própria.

Para prosseguir é preciso incluir o dispositivo onde foi instalado o sistema operacional na placa Raspberry Pi e *botar.* Com uma interface limpa e de fácil entendimento, prosseguir com a configuração utilizando um mouse e teclado plugado à placa. Após a inicialização do sistema operacional no Raspberry Pi, a placa está disponível para uso, contendo uma área desktop familiar para usuários de Windows, Linux ou mesmo Mac OS.

3.2.2 Vantagens do Raspberry Pi OS

O sistema oferece uma interface gráfica amigável e simples, permitindo que usuários com pouca experiência em linha de comando configurem e gerenciem o dispositivo com facilidade. Isso é especialmente útil em projetos que demandam monitoramento visual ou aplicativos que dependam de interfaces gráficas.

Inclui uma seleção de softwares úteis, como navegadores Web para acessar interfaces de configuração baseadas na Web e editor de texto, além de outros programas como ferramentas de programação, por exemplo Geany.

Como o sistema operacional vem com bibliotecas e pacotes adicionais pré-instalados, ele está pronto para implementar painéis gráficos de monitoramento ao tráfego de rede, usar ferramentas, como Wireshark, para análise de pacotes além de integrar aplicações para monitoramento de desempenho ou visualização de logs.

3.3 Iptables

O iptables é uma ferramenta poderosa usada em sistemas Linux para configurar, gerenciar e aplicar regras de firewall. Ele funciona no nível do kernel, que permite filtrar, redirecionar e monitorar o tráfego de rede que entra e sai do sistema.

Atua com base em uma série de regras organizadas em tabelas e cadeias. Cada pacote que passa pelo sistema pode ser filtrado com base nessas regras. As regras determinam o que fazer com os pacotes de dados, como aceitar, rejeitar ou redirecionar.

É uma interface de linha de comando para configurar o firewall no Linux, permite filtrar, redirecionar, bloquear ou permitir pacotes de rede com base em critérios como origem, destino, protocolo, porta e outros parâmetros.

3.3.1 Estrutura do Iptables

3.3.1.1 Tables (Tabelas)

O iptables contém diferentes tabelas, como informado na tabela 2, que agrupam as regras por função, cada uma destinada a um propósito específico:

Filter: A tabela padrão e mais usada, destinada ao controle de tráfego, determinando se os pacotes devem ser aceitos ou rejeitados.

Nat: Usada para traduzir endereços IP (NAT - *Network Address Translation*). É útil em roteadores e firewalls que realizam NAT.

Mangle: Utilizada para alterar as propriedades dos pacotes, como a definição de QoS (*Quality of Service*).

Raw: Permite alterar pacotes antes de serem processados por outras tabelas, usada principalmente para ajustar pacotes de conexão.

3.3.1.2 *Chains* (Cadeias)

Cada tabela contém cadeias que determinam a sequência pela qual as regras serão aplicadas:

INPUT: Para o tráfego que chega ao sistema local. Pacotes destinados ao próprio sistema são processados aqui.

FORWARD: Para pacotes que passam pelo sistema, mas são destinados a outras redes ou máquinas (usado em roteadores).

OUTPUT: Para o tráfego gerado pelo próprio sistema e que está saindo para a rede.

3.3.1.3 *Targets* (Alvos):

Após verificar uma regra, o iptables decide o que fazer com o pacote, baseando-se no target (alvo):

ACCEPT: O pacote é permitido a seguir seu caminho.

DROP: O pacote é descartado silenciosamente.

REJECT: O pacote é bloqueado, e uma mensagem de erro é enviada ao remetente.

LOG: O pacote é registrado no log do sistema, mas sua jornada continua.

DNAT e SNAT: Alteram o endereço de destino ou de origem, usado em regras de NAT.

Tabela 2: Estrutura Iptables

TABLE	CHAIN	INTERFACES	
		ENTRADA	SAIDA
FILTER	INPUT	SIM	NÃO
	FORWARD	SIM	SIM
	OUTPUT	NÃO	SIM
NAT	PREROUTING	SIM	NÃO
	POSROUTING	NÃO	SIM
	OUTPUT	NÃO	SIM
MANGLE	INPUT	SIM	NÃO
	FORWARD	SIM	SIM
	OUTPUT	NÃO	SIM
	PREROUTING	SIM	NÃO
	POSROUTING	NÃO	SIM

Fonte: De autoria própria

3.3.2 Principais Aplicações

3.3.2.1 Firewall

O iptables é frequentemente usado em projetos para proteger servidores e estações de trabalho, bloqueando tráfego indesejado e permitindo apenas o tráfego autorizado.

3.3.2.2 Roteamento e NAT

Usado em roteadores para realizar NAT (Network Address Translation), permitindo que várias máquinas em uma rede interna usem um único IP público para acessar a internet.

3.3.2.3 Rate Limiting

Rate limiting é uma estratégia que limita a frequência com que uma ação pode ser repetida em um determinado período. É uma medida de segurança que pode ser implementada em sites e aplicativos para proteger contas de usuários contra-ataques

de força bruta. Com iptables, é possível aplicar limites de taxa de requisições para evitar ataques de negação de serviço (DoS).

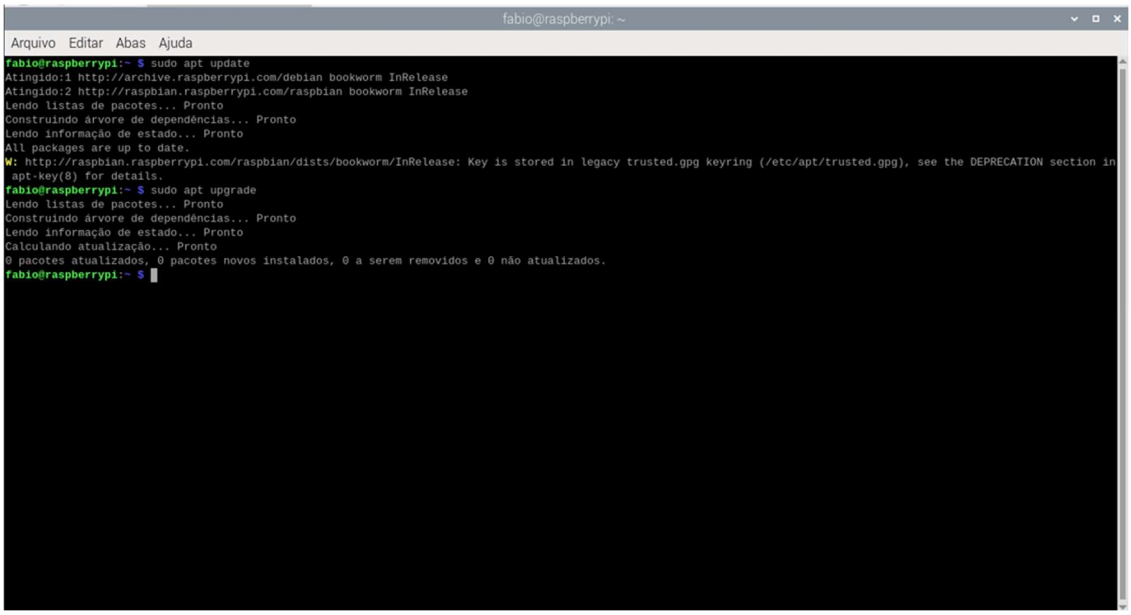
3.3.2.4 Monitoramento de Tráfego

O iptables permite registrar informações sobre pacotes que passam pelas regras configuradas usando o target LOG. Ao adicionar uma regra de log, pode-se gerar entradas detalhadas sobre o tráfego de rede.

4 Implementação de Regras

Na interface da Raspberry, todas as regras são implementadas por linhas de código no prompt de comando do Raspberry Pi OS. A princípio é feito a atualização de todo o sistema da placa, para assim obter as versões atuais, como descrito na figura 8.

Figura 8: Update e Upgrade do sistema

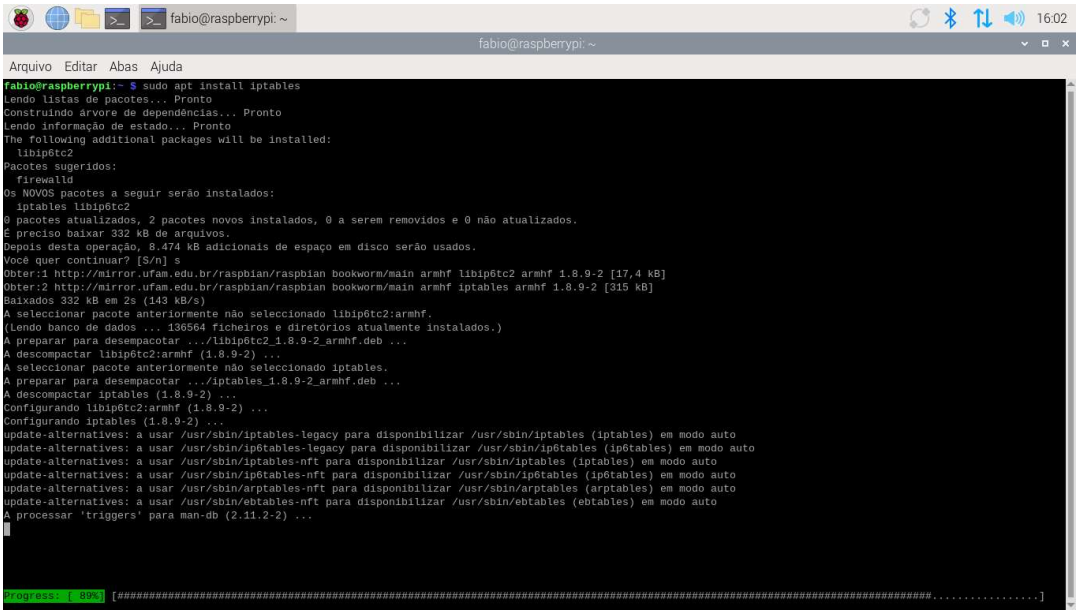


Fonte: De autoria própria.

Embora a maioria das distribuições Linux, incluindo o Raspberry Pi OS, já venha com o iptables instalado por padrão, em alguns casos pode ser necessário instalá-lo manualmente, especialmente após uma instalação limpa ou se o pacote tiver sido removido.

Para garantir que o iptables esteja instalado corretamente é preciso que a lista de pacotes esteja atualizada, como feito anteriormente. A figura 9 indica o processo de instalação do iptables.

Figura 9: Instalação do pacote Iptables



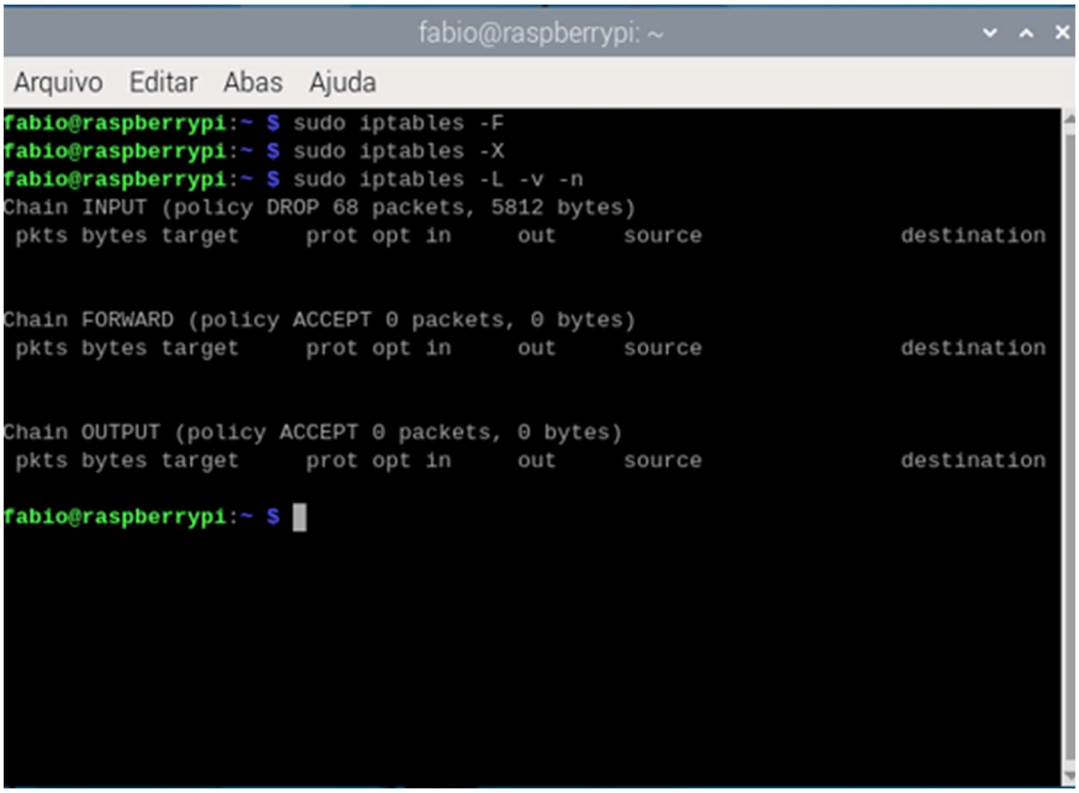
Fonte: De autoria própria.

Ao efetuar a instalação do pacote, pode-se começar a configurar as regras de firewall com iptables para proteger sua rede. A primeira etapa sempre deve ser limpar as regras existentes, ilustrado pela figura 10, antes de aplicar novas regras é importante confirmar que não há qualquer configuração anterior de regras de firewall para evitar conflitos.

A função -F limpa todas as regras.

A função -X remove tabelas personalizadas, caso existam.

Figura 10: Remoção de regras



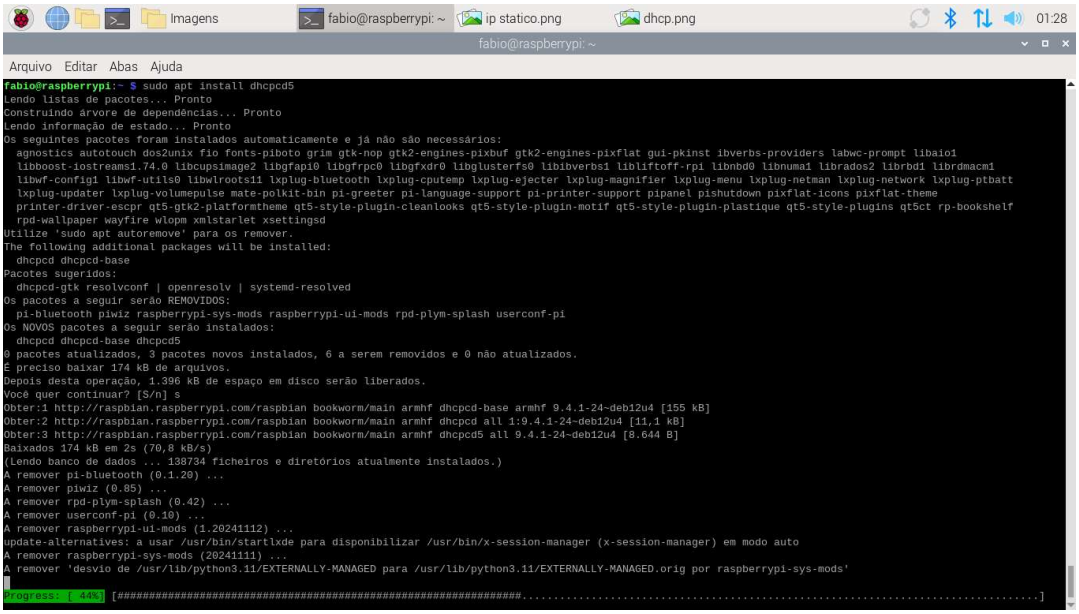
Fonte: De autoria própria.

É usado um único endereço de IP, sendo referente a rede cabeada ligada a Raspberry, com o intuito de evitar qualquer tipo de complicações futuras, faz-se a configuração para IP Estático.

Em dispositivos como firewalls, um endereço IP fixo, implantado pela regra apresentada nas figuras 11 a 13, é indispensável, pois outras máquinas na rede podem ter regras dependentes do endereço da Raspberry Pi e o roteador precisa saber para onde direcionar o tráfego.

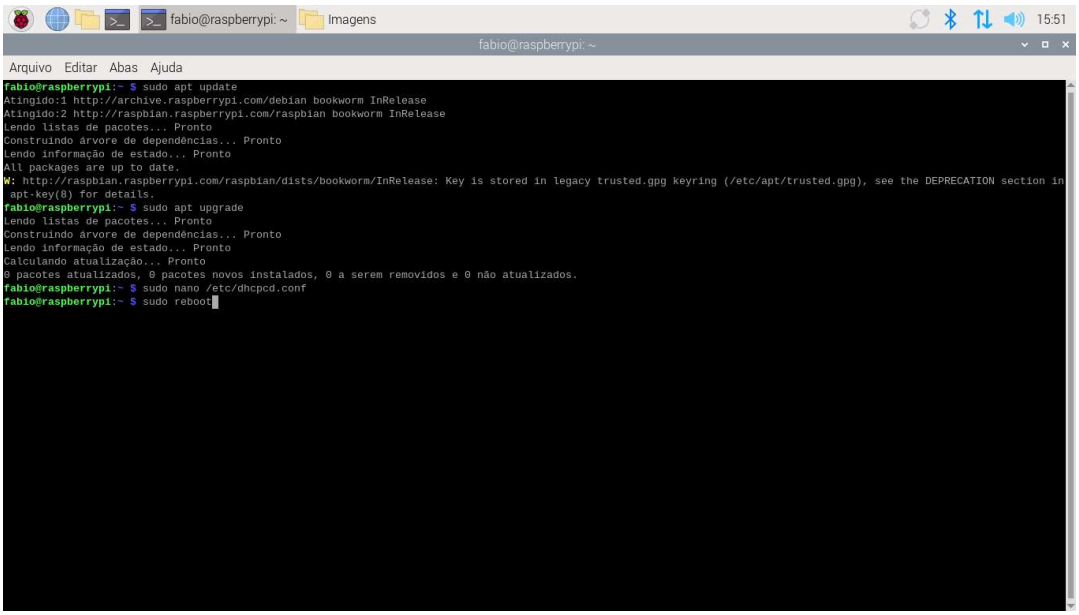
Ao fixar o IP, é possível evitar que o DHCP do roteador atribua o mesmo endereço IP a outro dispositivo, o que causaria conflitos. Em regras de iptables, redirecionamento de portas ou configurações de acesso remoto, o IP fixo garante que essas configurações não se tornem inválidas após uma reinicialização ou desconexão.

Figura 11 Instalação do pacote DHCP



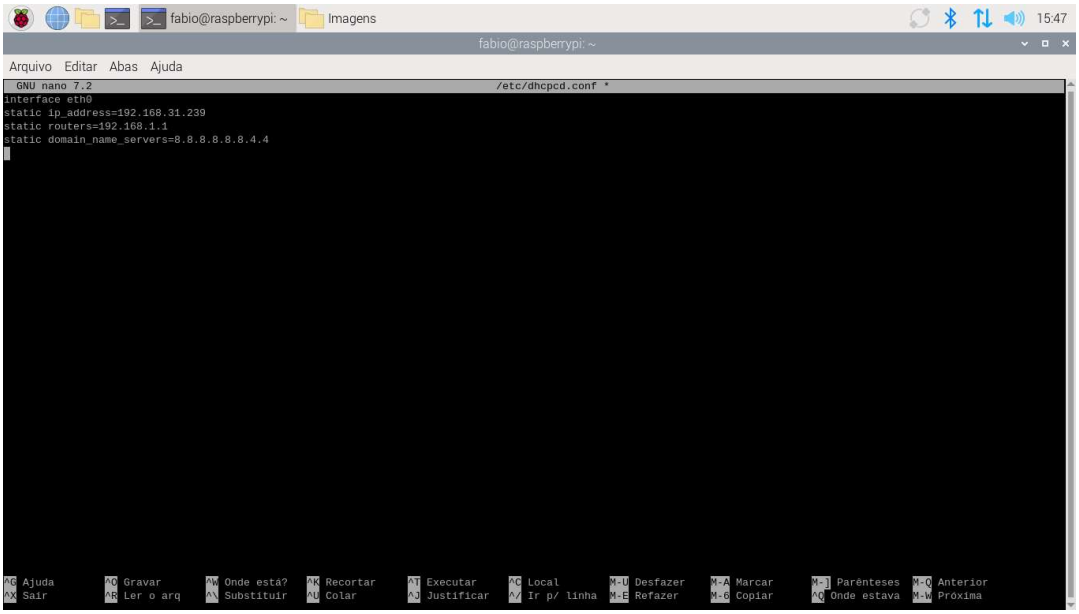
Fonte: De autoria própria.

Figura 12 Atualização e acesso ao painel DHCP



Fonte: De autoria própria.

Figura 13 Configuração do IP Estático



Fonte: De autoria própria.

Por se tratar de um ambiente de pequeno porte, as regras a serem estabelecidas podem ser bem especificas. No caso de bloqueio, o que for para ser bloqueado deverá ser explicito. Na figura 14 é definido a seguinte política padrão:

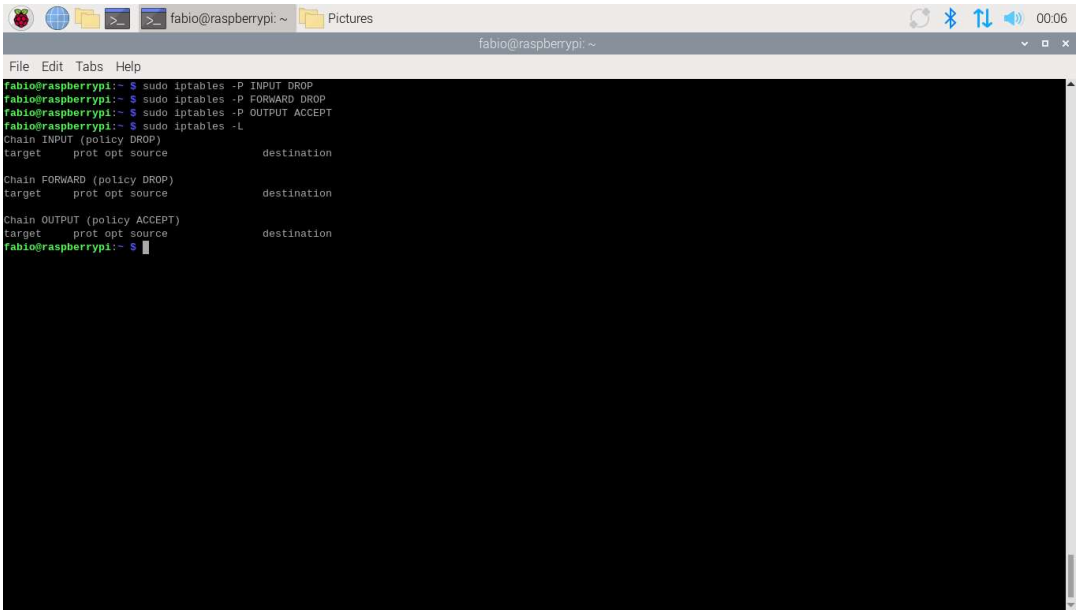
Política INPUT DROP: Isso significa que todo o tráfego de entrada será bloqueado por padrão, exceto quando explicitamente permitido por uma regra anterior. Isso é útil para proteger a Raspberry Pi de acessos indesejados de dispositivos externos.

Política FORWARD DROP: Bloquear o tráfego FORWARD significa que pacotes que atravessam a Raspberry Pi para outro dispositivo na rede serão barrados.

Política OUTPUT ACCEPT: Aceitar o tráfego OUTPUT garante que a Raspberry Pi consiga enviar pacotes para fora da rede, como acessar a internet para atualização do sistema e realizar testes de rede.

Levando em consideração que as regras voltadas a segurança serão implementadas após esse ponto, essa ação de deixar as cadeias sem restrições não é prejudicial.

Figura 14: Regras de política padrão

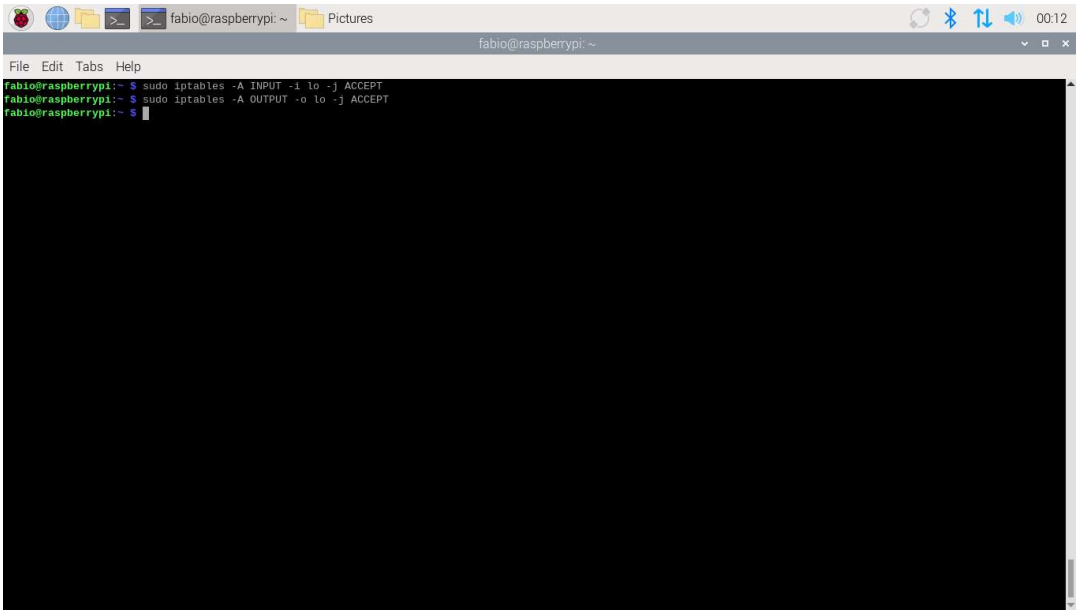


Com os procedimentos padrões e iniciais realizados, é possível focar em regras necessárias para o ambiente local. O tráfego local (localhost) precisa ser permitido para garantir que a Raspberry Pi possa se comunicar consigo mesma, por exemplo, para acessar serviços internos ou realizar testes de rede.

A interface lo é a interface de loopback e é configurada para o endereço IP 127.0.0.1. Assim, a figura 15 representam uma regra na cadeia INPUT que permite pacotes de entrada provenientes da interface de loopback (lo), permitindo que a Raspberry Pi se comunique internamente, e uma regra na cadeia OUTPUT que permite pacotes de saída para a interface de loopback, permitindo que a Raspberry Pi envie dados para si mesma.

Serviços ou aplicações que tentam se comunicar internamente podem não funcionar corretamente, levando a erros inesperados, por isso tal regra é de grande importância.

Figura 15: Definição de Tráfego Local (Localhost)



Fonte: De autoria própria

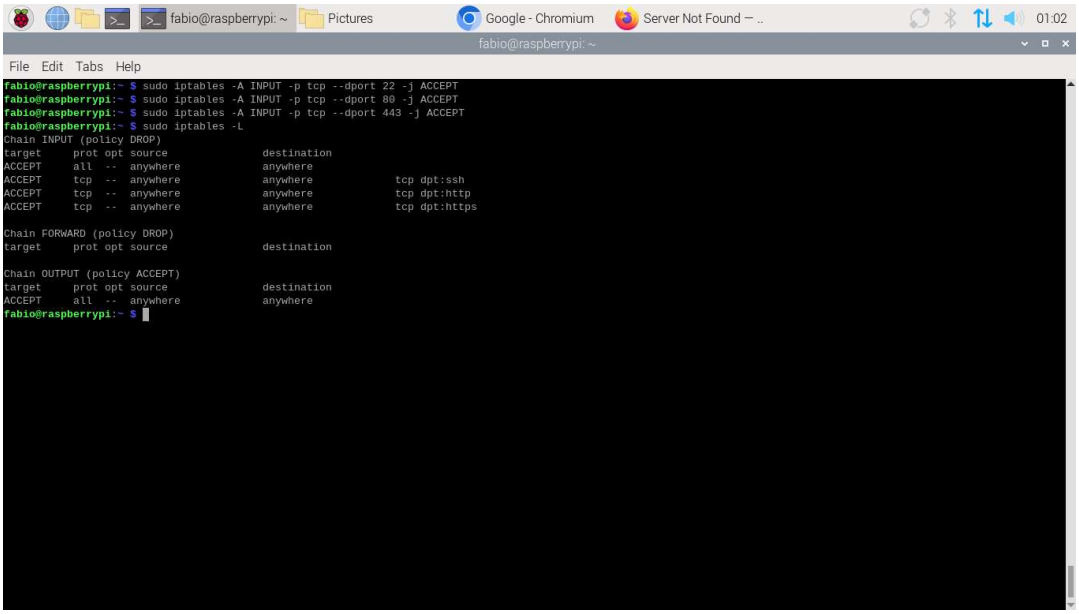
Bloquear o tráfego de entrada por padrão é uma prática de segurança fundamental, pois minimiza os pontos de entrada para ataques. Só o que for explicitamente permitido e necessário, será acessível.

Se não for configurado para bloquear por padrão, qualquer serviço que for iniciado na Raspberry Pi, intencionalmente ou por acidente, pode começar a aceitar conexões indesejadas.

Mesmo sistemas atualizados podem ter vulnerabilidades em softwares ou serviços. Bloquear o tráfego por padrão impede que *exploits*, técnica de vulnerabilidade, de serviços inseguros sejam acessíveis.

As regras indicadas na figura 16, bloqueando dados de entrada, garantem que somente o SSH (*Secure Shell*) para administração remota, sendo a porta 22, e os serviços Web HTTP/HTTPS, portas 80 e 443, sejam acessíveis, o que é uma abordagem eficiente.

Figura 16: Permissão SSH / HTTP / HTTPS



Fonte: De autoria própria

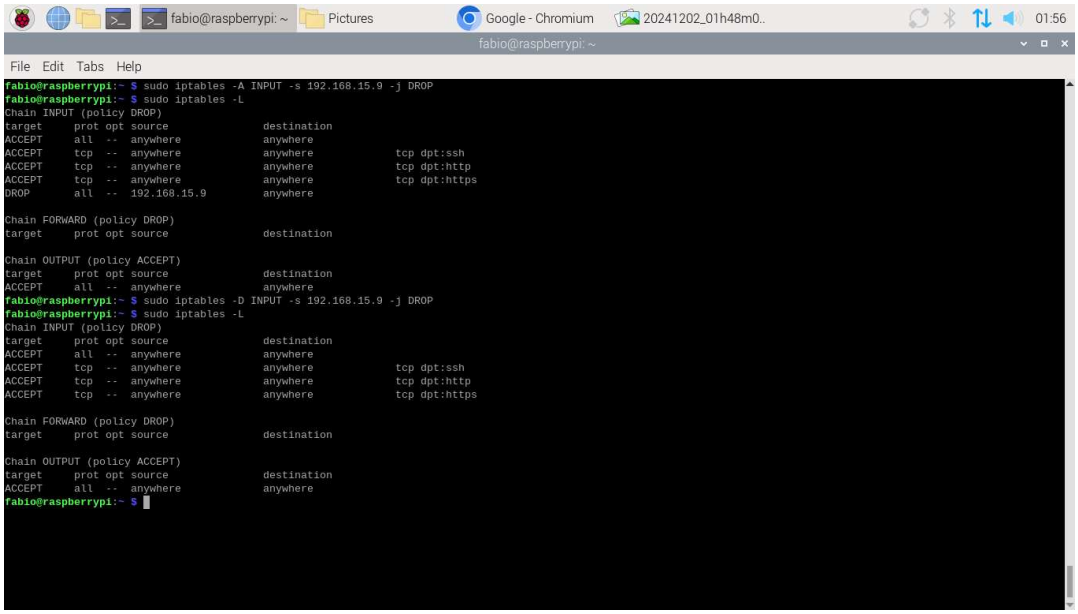
A regra de bloqueio de pacotes de entrada de IPs suspeitos, ilustrada na figura 17, é uma prática eficaz e simples de implementar para fortalecer a segurança de sistemas e redes.

Ao limitar o tráfego de fontes maliciosas, ela contribui para a estabilidade e proteção de ambientes computacionais, sendo especialmente relevante em infraestruturas críticas ou expostas à internet.

Tal regra tem como função bloquear o tráfego de fontes identificadas como maliciosas, como bots, scanners de portas ou atacantes que tentam explorar vulnerabilidades do sistema.

A primeira etapa mostrada na figura 17 retrata a criação da regra, sendo que o comando “sudo iptables -A INPUT -s 192.168.15.9 -j DROP” faz com que o dispositivo de tal ip não consiga se comunicar com a Raspberry Pi. A segunda etapa, representada pelo comando “sudo iptables -D INPUT -s 192.168.15.9 -j DROP” é uma demonstração de exclusão de regra, possibilitando alterações futuras caso necessário ter permissão ao dispositivo novamente.

Figura 17: Bloqueio IP específico.

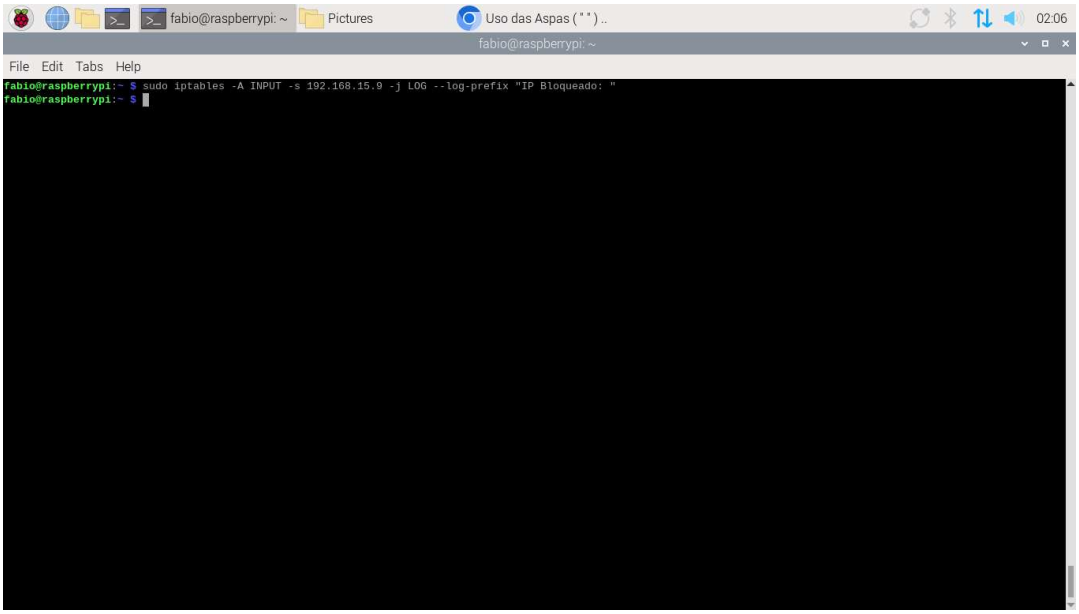


Fonte: De autoria própria.

Para complementar a regra onde é feito bloqueio de IP’s específicos, pode-se utilizar o controle de logs, que desempenha um papel essencial na segurança e na gestão da rede. Ele consiste em registrar eventos e atividades relacionadas ao tráfego que passa pelo firewall, como conexões permitidas, bloqueadas e possíveis tentativas de invasão.

Definir uma regra de controle de logs, figura 18, permite que os administradores acompanhem o que está acontecendo na rede em tempo real ou em retrospectiva, identificando padrões de tráfego e registrando conexões legítimas e tentativas suspeitas.

Figura 18: Registro de Log

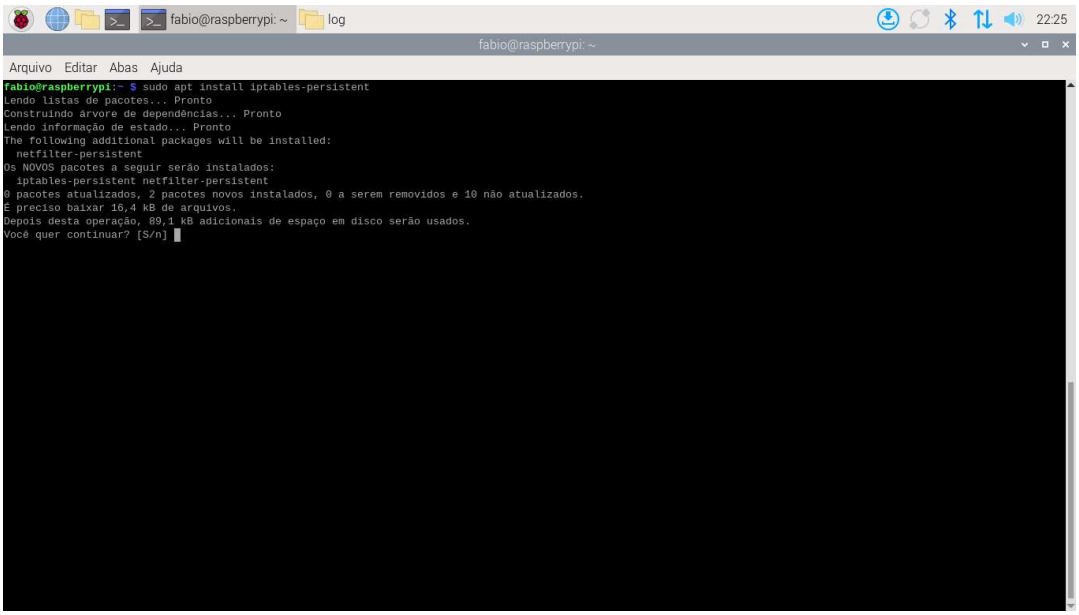


Fonte: De autoria própria

Após a finalização de todo o processo de criação de regras, permitindo ou negando tais situações, deve-se salvar as regras de uma forma que sejam mantidas futuramente independente de qualquer reinicialização.

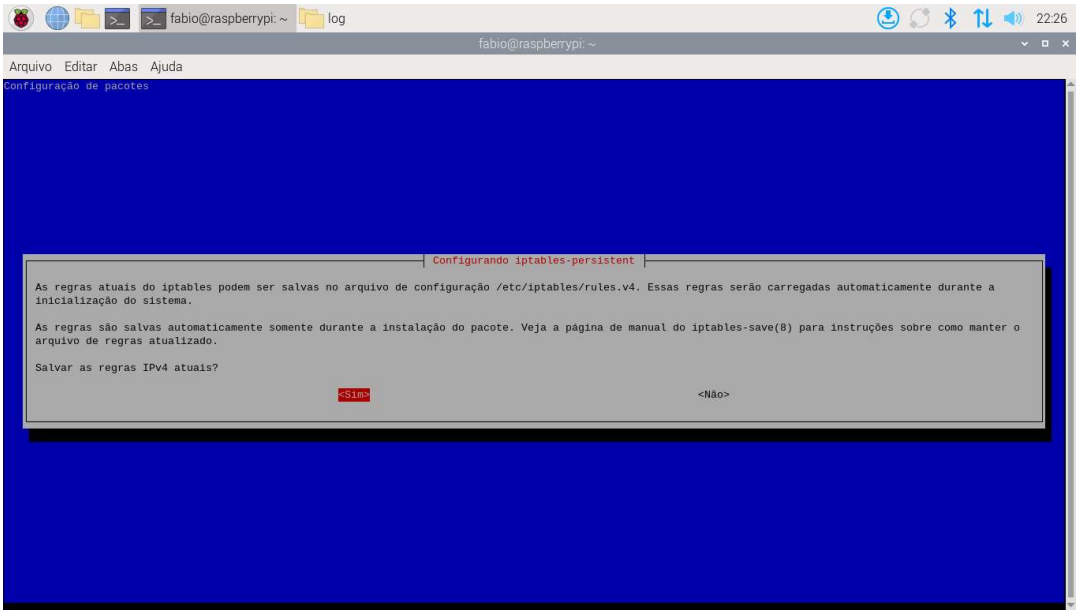
É possível efetuar o *save* automático a partir da instalação do pacote Persistent, voltado a salvamento das regras automático, ilustrado nas figuras 19 e 20.

Figura 19: Instalação do pacote Persistent



Fonte: De autoria própria.

Figura 20 Aviso de salvamento automático



Fonte: De autoria própria.

5 Análise de Resultados

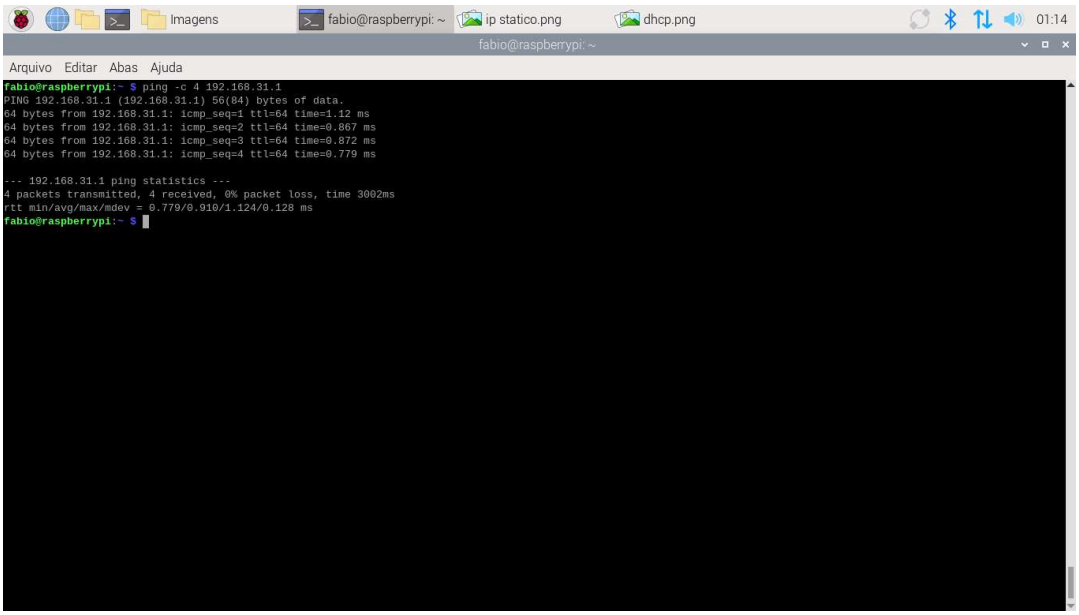
O presente capítulo é destinado à realização de testes das regras implementadas ao firewall, comprovando eficiência e funcionalidade, como descrito inicialmente no capítulo 4.

A figura 21 ilustra o comando ping que verifica se a Raspberry Pi está conseguindo se comunicar com o dispositivo de destino, neste caso, o IP 198.168.31.1 se refere ao roteador de internet utilizado. Ele envia 4 pacotes e aguarda as respostas. O resultado do comando indicará:

- Se os pacotes chegaram ao destino e retornaram.
- O tempo que cada pacote levou para ir e voltar, medido em milissegundos (ms).
- Se houver algum problema de conectividade, como o destino não estar acessível.

Resultado esperado: Conexão bem-sucedida, todos os pacotes são enviados e recebidos com sucesso, mostrando o tempo de ida e volta.

Figura 21: Teste DHCP junto ao reteador de internet



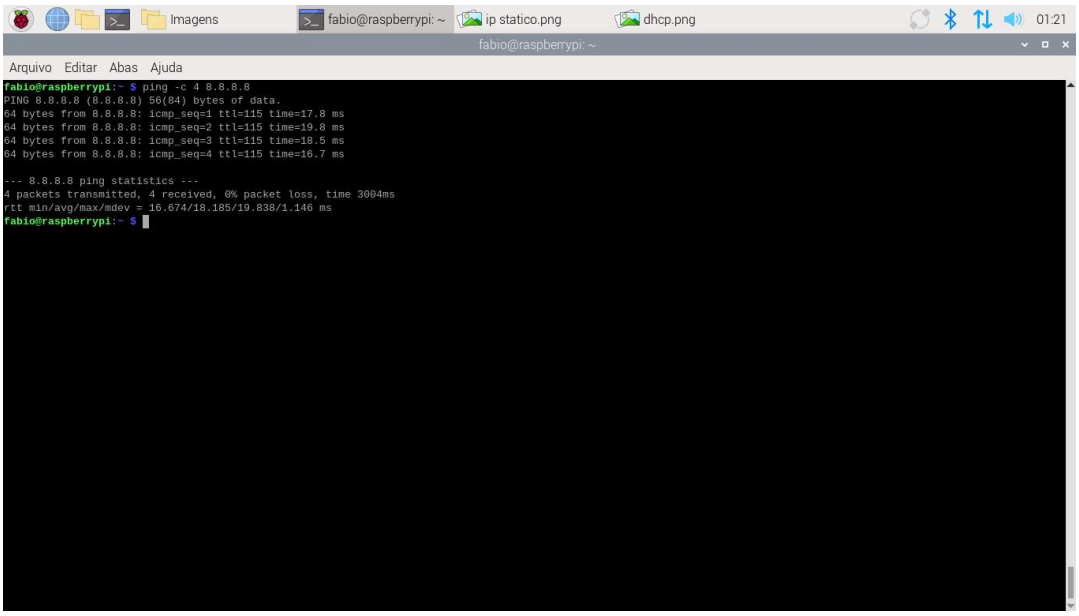
Fonte: De autoria própria

O comando ping é usado para verificar se a Raspberry Pi consegue se comunicar com o servidor DNS do Google (8.8.8.8). Se a conexão estiver funcionando corretamente, o servidor responderá aos pacotes enviados pela Raspberry Pi, e o tempo de ida e volta dos pacotes será registrado.

Objetivo do Teste: verificar a conectividade da Raspberry Pi com a internet, utilizando um servidor público confiável (Google DNS).

O comando envia 4 pacotes para o IP 8.8.8.8, que é o servidor DNS do Google. Ele aguarda as respostas e calcula o tempo de ida e volta dos pacotes. Os pacotes são recebidos com sucesso, provando que a Raspberry Pi está conectada à internet.

Figura 22: Teste de conexão ao IP do Google



Fonte: De autoria própria

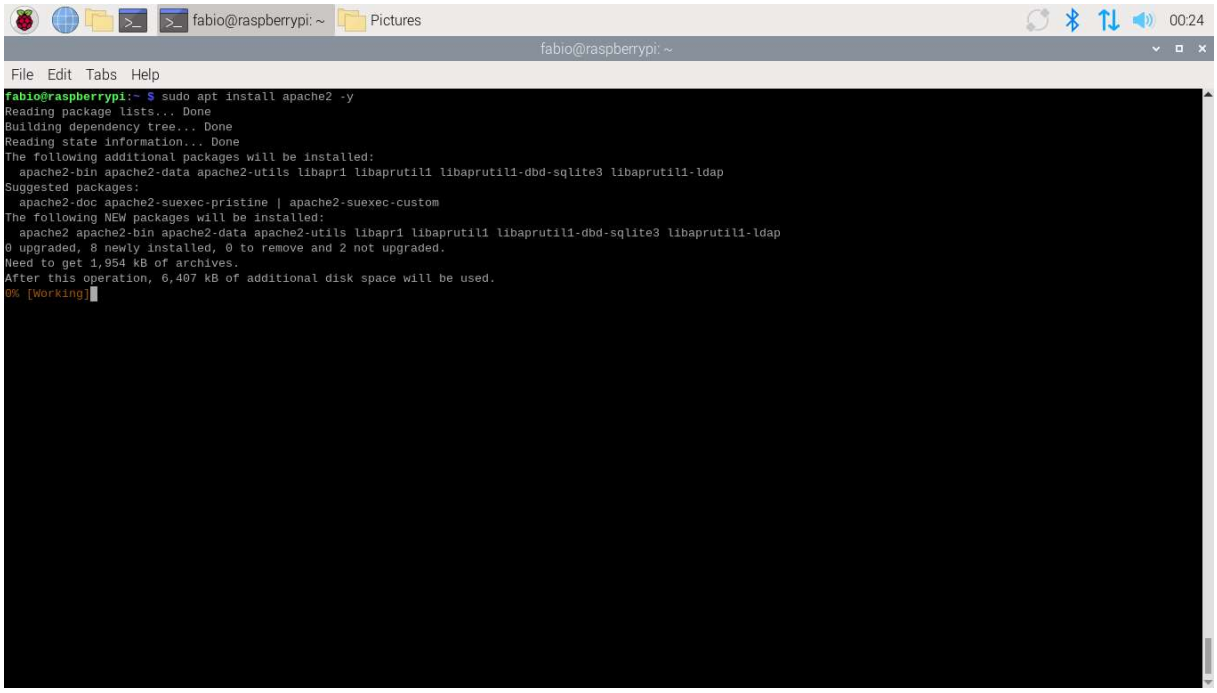
Após a verificação de conexão DHCP e conexão de internet, é iniciada a fase de testes de conexão local da Raspberry. Durante a implementação das políticas padrões, foi definido e demonstrado na lista de exibições de regras que o *firewall* rejeita tráfegos de entrada e tráfegos que passem pela placa, permitindo apenas tráfego de saída.

Porém a implementação da regra de localhost na cadeia INPUT representa a permissão de pacotes de entrada provenientes da interface de loopback (lo), permitindo que a Raspberry Pi se comunique internamente.

A interface de loopback (lo) é uma interface virtual na qual a máquina se comunica consigo mesma. Quando se enviam dados para o endereço 127.0.0.1, esses dados não saem da máquina, mas são processados internamente.

Para um teste mais preciso, além da utilização do ping para verificar funcionalidade, é feito a instalação do pacote de um servidor Web chamado apache, ilustrado pela figura 23.

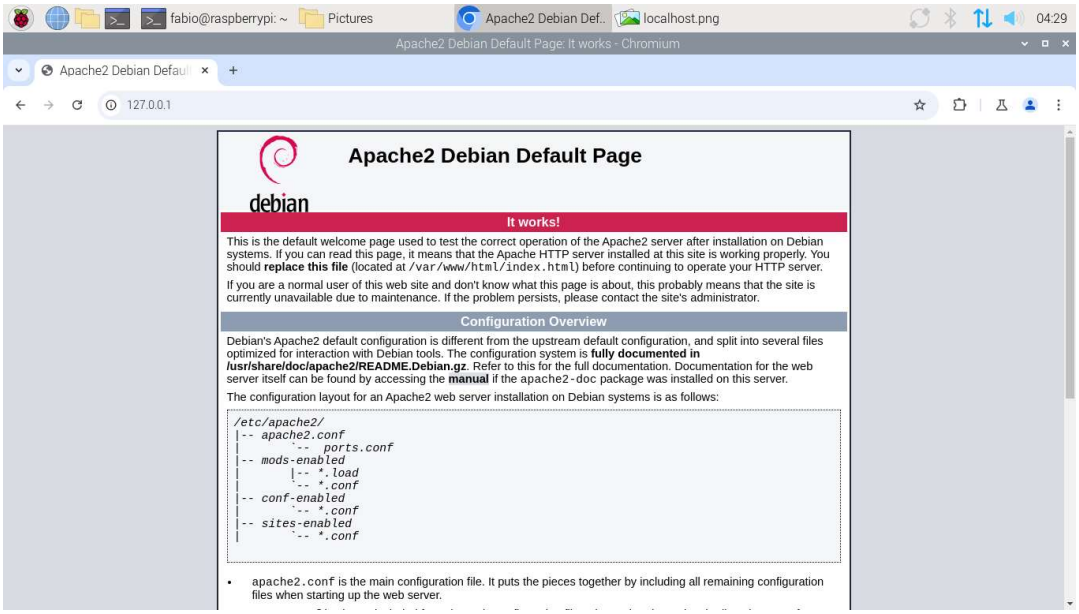
Figura 23: Instalação pacote servidor Web



Fonte: De autoria própria

O teste efetuado na figura 24 apresenta a comunicação interna da placa, devido a regra de localhost implementada. Sendo retratada pela interface gráfica do servidor Web, provando conexão simbolizada por “*It Works*”, ou seja, a regra está em operação.

Figura 24: Teste localhost junto ao servidor Web apache



Fonte: De autoria própria

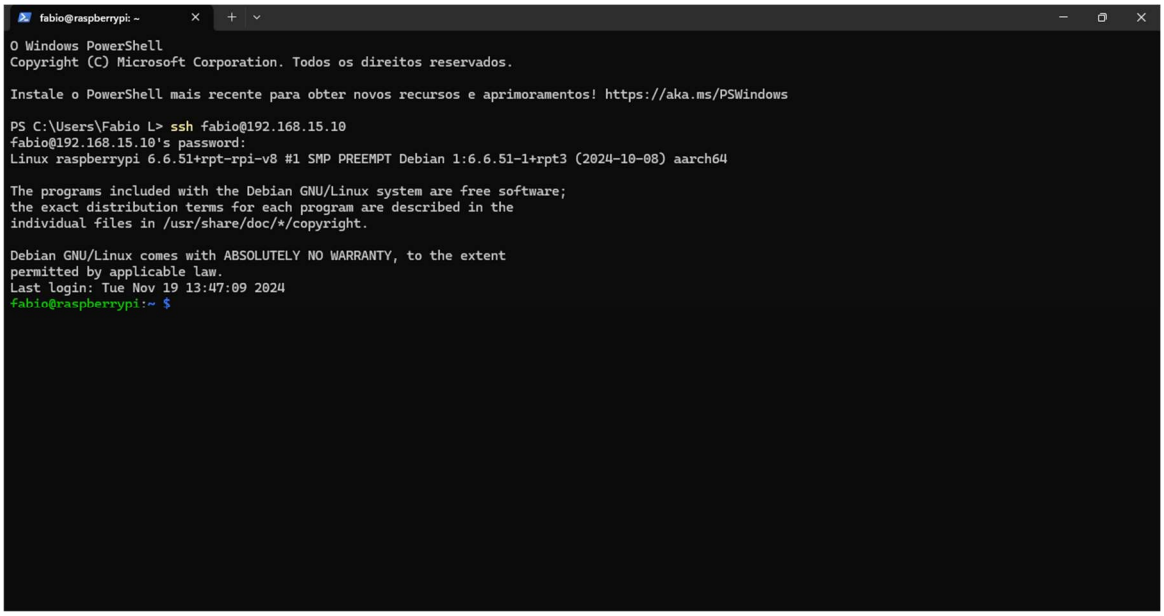
Com o servidor Web, se torna possível também efetuar os testes de conexão de outro dispositivo local junto a Raspberry Pi.

A figura 25 demonstra conexão de um outro dispositivo, com sistema operacional Windows 11, se conectando a Raspberry Pi via SSH (*Secure Shell*). Para essa conexão funcionar, é preciso ter a regra implementada pela figura 16, a qual da a devida permissão.

Em outro dispositivo é aberto a interface do Windows PowerShell e inserido o comando para conectar a ‘NomeDaRaspberry@IPRaspberry’, após isso é solicitado a senha definida para Raspberry.

Resultado esperado: A regra foi configurada corretamente, a conexão SSH é estabelecida, permitindo o acesso remoto.

Figura 25: Conexão remota com outro dispositivo

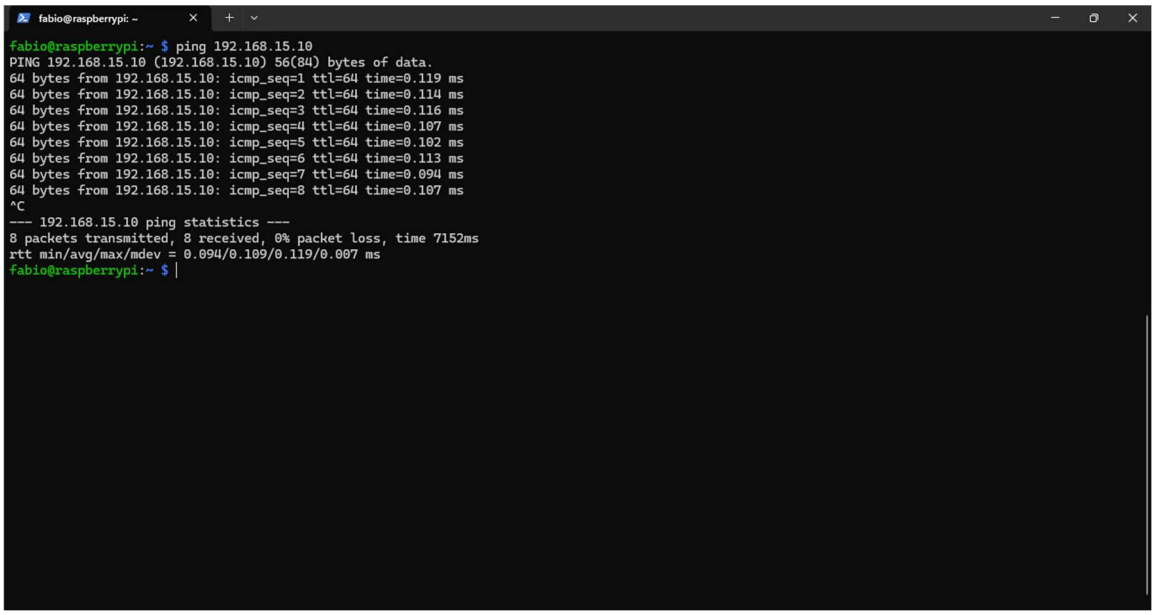


Fonte: De autoria própria

Concluída a conexão remota, é efetuado o teste da regra de permissão a porta 80 e porta 442 (HTTP e HTTPS), sendo realizado juntamente ao servidor Web apache.

Ainda sendo efetuado pelo outro dispositivo e conectado remotamente, é efetuado o teste de ping ao IP da placa Raspberry, ilustrado pela figura 26.

Figura 26: Ping ao IP da Raspberry via dispositivo remoto

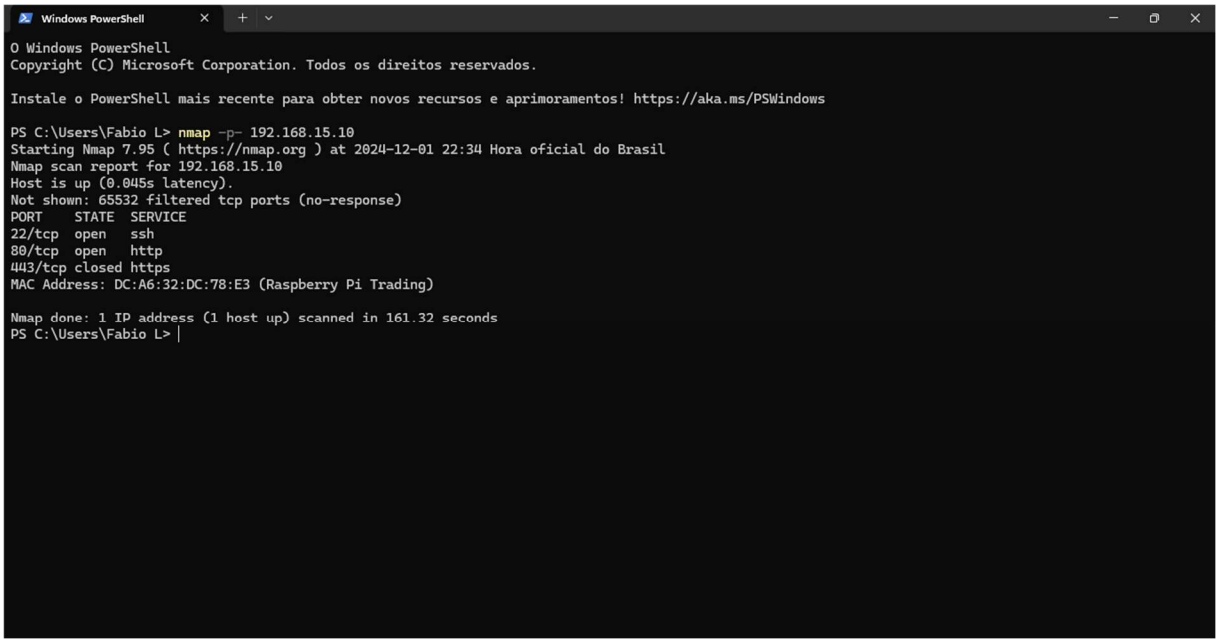


Fonte: De autoria própria

A fim de comprovar a funcionalidade da conexão remota, é feita a instalação de um programa externo, chamado nmap, capaz de efetuar o escaneamento de portas.

A figura 27 apresenta o scaner em funcionamento, informando o *status* das portas 22 (SSH), 80 (HTTP) e 443 (HTTPS).

Figura 27: Escaneamento de portas com Nmap



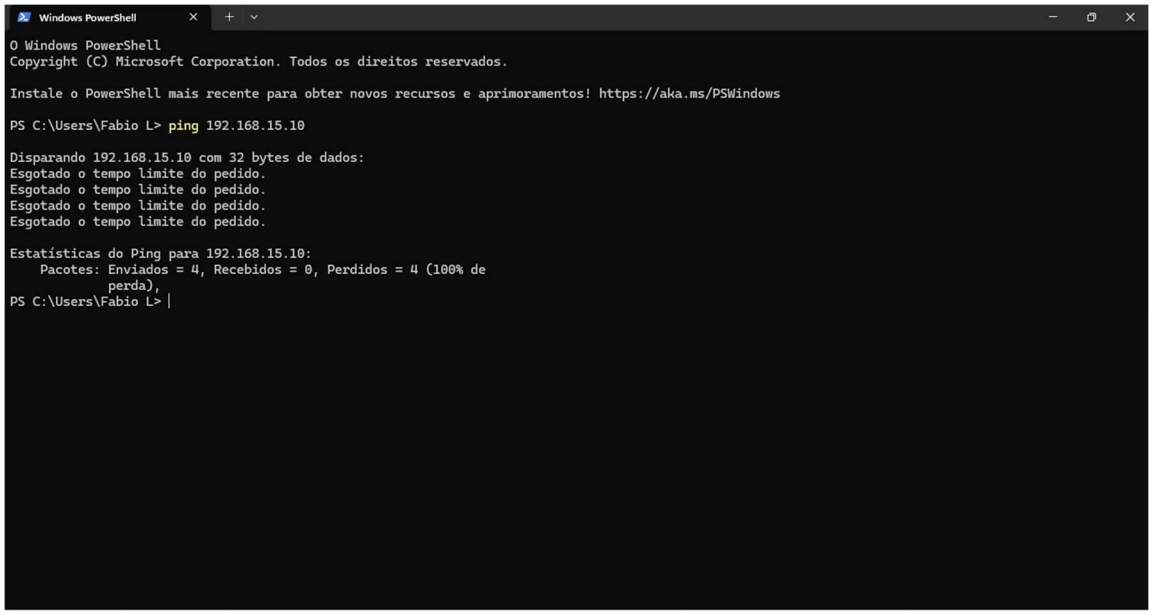
Fonte: De autoria própria

A regra apresentada pela figura 17 para bloqueio de IP específico (sudo iptables -A INPUT -s 192.168.15.9 -j DROP) tem como objetivo bloquear o tráfego de entrada proveniente de um IP específico (neste caso, 192.168.15.9).

Na figura 28 é possível ver o dispositivo com o IP 192.168.15.9, efetuando ping para o ip da placa, o qual é barrado devido a restrição aplicada pela regra.

Resultado esperado: sucesso da regra, o comando ping falha com a mensagem "Esgotado o tempo limite do pedido" ou equivalente, indicando que os pacotes foram descartados.

Figura 28: Teste remoto de conexão a placa negado



Fonte: De autoria própria

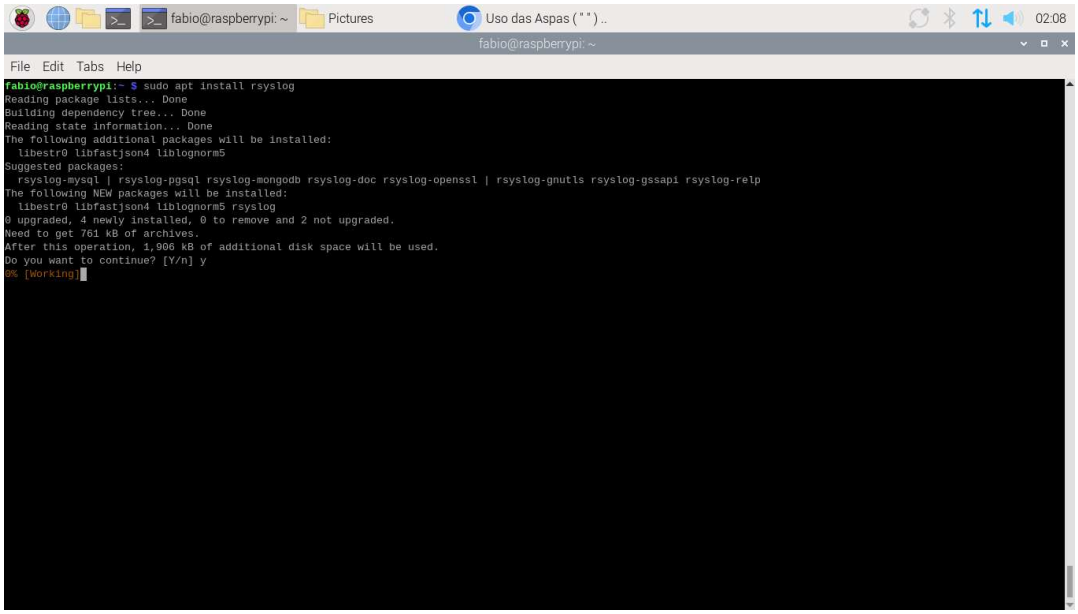
Com o bloqueio de IP's específicos, é também necessário fazer o devido monitoramento. Adicionar uma regra de log ao firewall é uma prática fundamental para monitorar eventos relacionados ao tráfego de rede, como pacotes bloqueados ou conexões suspeitas. A regra apresentada na figura 18 registra os pacotes de entrada do IP 192.168.15.9 antes de descartá-los. Sendo necessário o pacote syslog, já pré-instalado no Raspberry Pi OS, é feito a ativação desse pacote pelo comando ilustrado na figura 29.

O comando de teste apresentado pela figura 30 permite que administradores acompanhem o comportamento da rede em tempo real ou realizem análises futuras.

Objetivos da Regra:

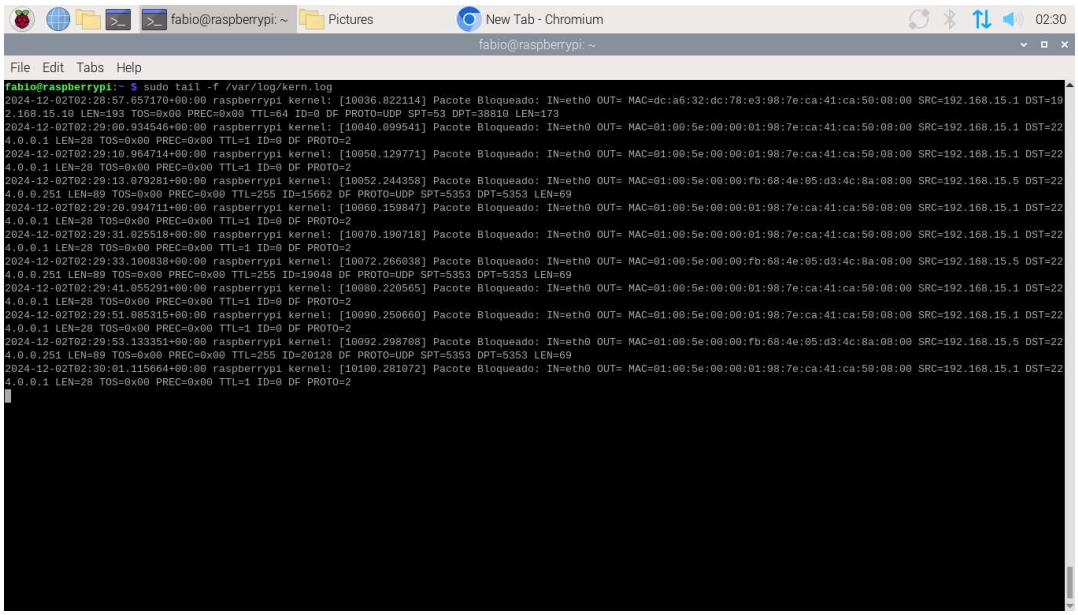
- Registrar tentativas de conexão de um IP bloqueado (192.168.15.9), gerando logs detalhados para análise.
- Auxiliar na identificação de padrões de tráfego suspeitos ou maliciosos.
- Criar um histórico de eventos para auditorias ou investigações futuras.

Figura 29: Instalação do pacote de registro dos Log’s



Fonte: De autoria própria

Figura 30: Registro de Log’s



Fonte: De autoria própria

6 Considerações Finais

Após os tópicos apresentados, infere-se na conclusão de que o trabalho é viável e trará bons frutos. Este projeto foca no estudo de regras de *firewall* em ambientes de pequeno porte, onde utilizará uma abordagem prática com o uso de um Raspberry Pi 4.

Inicialmente, é abordado a importância dos *firewall*s na segurança de redes, destacando suas funções principais, dando um maior entendimento na área. É discutido sobre *firewalls* e suas respectivas funcionalidades, além de detalhar como as regras de *firewall* podem ser configuradas para atender às necessidades específicas de uma rede de pequeno porte.

Este trabalho visa ampliar a compreensão sobre as funcionalidades de um *firewall* e investigar as possibilidades de usar um Raspberry Pi como plataforma para segurança de rede. Adicionalmente, é fundamental ressaltar a importância da adoção de medidas de segurança em ambientes de Internet das Coisas (IoT), especialmente em Computadores de Placa Única (SBCs), para assegurar a proteção dos dispositivos e a integridade dos dados que circulam na rede.

Na pesquisa experimental, é demonstrado a utilização de um Raspberry Pi 4 como *firewall*, um dispositivo econômico e de fácil configuração. São aplicadas regras de filtragem de pacotes e configurações de rede que mostraram ser eficazes na proteção e gerenciamento do tráfego de rede.

O trabalho também analisa a importância dos princípios de segurança da informação, como confidencialidade, integridade e disponibilidade, destacando como os *firewall*s contribuem para garantir esses princípios em uma rede.

Através das análises e testes realizados, conclui-se que a implementação de *firewalls* em redes de pequeno porte é não apenas viável, mas também essencial para garantir a segurança e o desempenho da rede. O uso de dispositivos como o Raspberry Pi 4 oferece uma solução acessível e eficiente, tornando possível a proteção de redes menores sem a necessidade de investimentos significativos em *hardware* ou *software* caros.

Portanto, este estudo contribui significativamente para o campo da segurança de redes em ambientes de pequeno porte, fornecendo orientações práticas e comprovadas para a implementação de *firewall*s eficazes. Os resultados obtidos

mostram que, com as configurações corretas, mesmo redes menores podem alcançar um nível elevado de segurança, minimizando riscos e garantindo a proteção de dados e sistemas.

O uso de dispositivos como o Raspberry Pi 4 oferece uma solução acessível e eficiente, tornando possível a proteção de redes menores sem a necessidade de investimentos significativos em hardware ou software caros. Este estudo contribui significativamente para o campo da segurança de redes em ambientes de pequeno porte, fornecendo orientações práticas e comprovadas para a implementação de firewalls eficazes.

Os resultados obtidos mostram que, com as configurações corretas, mesmo redes menores podem alcançar um nível elevado de segurança, minimizando riscos e garantindo a proteção de dados e sistemas. O projeto reforça que a segurança de rede é uma questão prioritária e, com ferramentas acessíveis e conhecimento adequado, pode ser implementada de forma eficaz em qualquer ambiente.

No anexo 1 apresenta-se o termo de autorização para publicação.

6.1 Trabalhos Futuros

Propõe-se em trabalhos futuros:

- Interligação de múltiplos dispositivos ao *firewall.*
- Exploração de conexão via SSH para administrar o firewall remotamente.
- Implementação de regras utilizando mais de um IP, por exemplo IP Wi-Fi e IP Ethernet

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27032:2012 - Tecnologia da informação - Técnicas de segurança - Diretrizes para cibersegurança. Rio de Janeiro, 2012.

CORDEIRO, HEBERT. TRABALHO DE CONCLUSÃO DE CURSO – IMPLANTAÇÃO DE FIREWALL EM RASPBERRY PI. 2023.

GIL, ANTONIO CARLOS. COMO ELABORAR PROJETOS DE PESQUISA. 4 ED, 2017.

HINTZBERGEN, KESS; et al. - FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO: COM BASE NA ISO 27001 E NA ISO 27002. 1ª ED. 2018.

KANAGACHIDAMBARESAN, G. R. Papel dos Computadores de Placa Única (SBCs) na Prototipagem Rápida de IoT. Springer, 2021.

KUROSE, JAMES F. e ROSS, KEITH W. - REDES DE COMPUTADORES E A INTERNET. 6ª ED. 2013.

MENDES, DOUGLAS ROCHA. REDES DE COMPUTADORES: TEORIA E PRÁTICA. 2ª ED. 2016.

NAKAMURA, EMILIO e GEUS, PAULO – SEGURANÇA DE REDES EM AMBIENTES COOPERATIVOS 1ª ED. 2007.

NEWCOMB, Aaron. Linux for Makers: Understanding the Operating System That Runs Raspberry Pi and Other Maker SBCs. Maker Media, Inc, 2017.

STALLING, WILLIAM. SEGURANÇA DE COMPUTADORES 2 ED, 2014

TANENBAUM, ANDREW S.; WETHERALL, DAVID. - REDES DE COMPUTADORES - 5ª ED. 2011.

WAZLAWICK, RAUL SIDNEI. METODOLOGIA DE PESQUISA PARA CIENCIA DA COMPUTAÇÃO 2ªED. 2014.

ANEXO 1 - 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 n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante Fabio Aparecido Loiola Silva Junior do Curso de Engenharia de Computação, matrícula 2018.2.0033.0008-0, telefone: (62) 99853-1250 e-mail fabioalsj@hotmail.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 ESTUDO DE REGRAS DE FIREWALL PARA AMBIENTES DE PEQUENO PORTE, 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, 10 de setembro de 2024.

Assinatura do autor: Fábio A. Loiola S. Júnior

Nome completo do autor: Fabio Aparecido Loiola Silva Junior

Assinatura do professor–orientador: _____

Nome completo do professor-orientador: Marcelo Antonio Adad de Araujo