FIEL – FACULDADES INTEGRADAS EINSTEIN DE LIMEIRA

GRADUAÇÃO EM TECNOLÓGICO EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

Caike Alexandrino dos Santos  
João Vittor Domingos de Jesus

SEGURANÇA A NÍVEL DE REDE DOMÉSTICA: RASPBERRYPI & PI-HOLE

LIMEIRA, SP  
2024

Caike Alexandrino dos Santos  
João Vittor Domingos de Jesus

SEGURANÇA A NÍVEL DE REDE DOMÉSTICA: RASPBERRYPI & PI-HOLE

Monografia apresentada às Faculdades Integradas Einstein de Limeira – FIEL, como exigência parcial para obtenção do grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Orientador: Jonas Henrique Ferreira

LIMEIRA, SP  
2024

FIEL – FACULDADES INTEGRADAS EINSTEIN DE LIMEIRA

TERMO DE APROVAÇÃO

SEGURANÇA A NÍVEL DE REDE DOMÉSTICA: RASPBERRYPI & PI-HOLE

Caike Alexandrino dos Santos  
João Vittor Domingos de Jesus

Orientador Professor Esp Jonas Henrique Ferreira

Banca examinadora:

Professor Dr. Pedro Ivo Garcia Nunes

Professor Me. Johanny Tetzner

Professor Esp. Jonas Henrique Ferreira

Data de aprovação: 20/06/2024

Dedicatória

À nossa família, pelo amor, apoio incondicional e compreensão durante esta jornada.

# RESUMO

Uso de um Raspberry Pi com Pi-hole e Tailscale sendo uma VPN para proteger a rede doméstica. O objetivo era garantir uma navegação segura e privada, bloqueando rastreadores e anúncios. O Pi-hole efetivamente bloqueou sites indesejados. Apesar de alguns desafios iniciais, a configuração final demonstrou confiabilidade e eficácia, mostrando como essas tecnologias podem melhorar a segurança da rede doméstica.

**Palavras-chave:** 1. Raspberry Pi 2. Pi-hole 3. VPN

# SUMÁRIO

[RESUMO 8](#_Toc169188840)

[SUMÁRIO 9](#_Toc169188841)

[1 INTRODUÇÃO 10](#_Toc169188842)

[2 REVISÃO DE LITERATURA 11](#_Toc169188843)

[2.1.1 VPN 11](#_Toc169188844)

[2.1.2 RASPBERRY PI 12](#_Toc169188845)

[2.1.3 PI-HOLE 13](#_Toc169188846)

[2.2 Referencial teórico 14](#_Toc169188847)

[2.2.1 Citação indireta 15](#_Toc169188848)

[2.3 Trabalhos correlatos 16](#_Toc169188849)

[2.3.1 “Securing Network Using Raspberry Pi by Implementing VPN, Pi-Hole, and IPS (VPiSec)” 16](#_Toc169188850)

[2.3.2 "SafeSearch: Obfuscated VPN Server using Raspberry Pi for Enhancing User Privacy". 16](#_Toc169188851)

[3 MATERIAIS E MÉTODOS 16](#_Toc169188852)

[3.1.1 INSTALAÇÃO 16](#_Toc169188853)

[4 RESULTADOS 20](#_Toc169188854)

[5 CONCLUSÃO 23](#_Toc169188855)

[5.1 Trabalhos futuros 24](#_Toc169188856)

[REFERÊNCIAS 25](#_Toc169188857)

# INTRODUÇÃO

A crescente preocupação com a segurança e privacidade nas redes digitais sublinha a necessidade urgente de soluções robustas para proteger os usuários contra uma variedade de ameaças cibernéticas. Aqueles que utilizam redes insuficientemente seguras correm o risco de encontrar sérios problemas que comprometem sua experiência on-line e segurança pessoal. A ameaça persistente de malware e vírus em redes não seguras pode levar a ataques que infectam dispositivos, comprometem a integridade dos dados e perturbam as operações do sistema.

Além disso, os perigos do phishing e da fraude são substanciais, com os perpetradores usando táticas de engenharia social para enganar os usuários em divulgar informações confidenciais, como senhas e detalhes bancários, resultando em perdas financeiras significativas e aumento dos incidentes de roubo de identidade. Os atacantes frequentemente interceptam dados pessoais como nomes, endereços e números de telefone em redes vulneráveis, contribuindo para um aumento de atividades fraudulentas e casos de roubo de identidade, como transações não autorizadas e fraude de identidades. Redes sem medidas de segurança suficientes são suscetíveis a ataques de força bruta, onde os atacantes tentam quebrar senhas para obter acesso não autorizado a contas e dispositivos. Além disso, os anunciantes e os rastreadores exploram dados de usuários, monitorando secretamente as atividades on-line, coletando informações extensivas sobre o comportamento de navegação e potencialmente comprometendo a privacidade dos usuários.

Além de ameaças de segurança diretas, a presença de anúncios maliciosos e scripts em redes não seguras resulta em desempenho degradado com consumo excessivo de largura de banda e recursos de dispositivo, causando uma experiência de navegação lenta e ineficiente. Problemas como redirecionamento malicioso, onde os usuários são levados para sites fraudulentos que instalam malware ou coletam informações pessoais, também são comuns. Os ataques de negação de serviço (DoS) podem sobrecarregar os servidores e tornar os serviços legítimos inacessíveis, enquanto a mineração de criptomoedas não autorizada utiliza os recursos do dispositivo sem o consentimento do usuário. Extorsão e ransomware são ameaças alarmantes onde os atacantes criptografam os arquivos dos usuários e exigem um resgate pela chave de descriptografia, levando à perda de dados e custos financeiros. Além disso, ataques man-in-the-middle (MitM) permitem que os atacantes interceptem e manipulem a comunicação entre duas partes, comprometendo a confidencialidade dos dados e a integridade das transações on-line, comprometendo assim a segurança geral das redes.

Diante dessas preocupações, este trabalho propõe uma análise detalhada das ameaças enfrentadas pelos usuários de domésticas inseguras, e a apresentação de uma solução eficaz através da combinação de VPN e Pi-hole. Essa combinação surge como uma solução abrangente para mitigar essas ameaças. A VPN protege dados sensíveis em redes públicas, criptografando comunicações e garantindo que informações confidenciais permaneçam seguras. Junto com o Pi-hole, que bloqueia acessos a domínios associados a malware, phishing e outros tipos de conteúdos maliciosos, reduzindo a exposição a ameaças.

A VPN também permite que os usuários acessem conteúdo geograficamente restrito, contornando a censura e restrições. Além disso, impede o monitoramento por ISPs(Internet Service Providers) e protege contra ataques MitM(Main-In-The-Middle). O Pi-hole bloqueia os rastreadores de terceiros, preservando a privacidade dos usuários, impedindo o rastreamento de seus movimentos na web. Nas transações on-line, a VPN garante que os dados bancários sejam criptografados e protegidos contra interceptação, enquanto o Pi-hole reduz a exposição a anúncios direcionados, bloqueando-os ao nível da rede. A implementação destas tecnologias não só protege contra falsificação de DNS e análise de tráfego, mas também preserva o anonimato on-line, protege as comunicações pessoais e melhora a segurança digital geral para os usuários.

O uso destas tecnologias adiciona um grau extra de segurança que é necessário para reduzir os riscos e garantir uma experiência online produtiva e segura. O objetivo deste esforço é fornecer uma solução realista e eficaz que melhore a segurança e a privacidade em ambientes digitais, abordando substancialmente as preocupações dos usuários.

# REVISÃO DE LITERATURA

### VPN

Uma VPN (rede virtual provada) é uma tecnologia que permite a criação de uma conexão segura e criptografada através de uma rede intrinsecamente insegura, como a Internet pública. A VPN estabelece um túnel criptografado entre o dispositivo do usuário e o servidor VPN, protegendo os dados transmitidos contra intercepções e acesso não autorizado.

O principal objetivo de uma VPN é fornecer segurança e privacidade para os usuários durante a navegação on-line. Ao criptografar os dados, a VPN impede que terceiros, como hackers ou ISPs (provedores de serviços de Internet), monitorem ou recolham informações confidenciais. Além disso, a VPN pode melhorar a privacidade e habilitar a navegação anônima, mascarando o endereço IP do usuário com o IP do servidor VPN.

As VPNs são amplamente utilizadas em diversos contextos, como em ambientes corporativos e para necessidades pessoais de navegação. No ambiente corporativo, as VPNs permitem que os funcionários acessem de forma segura a rede da empresa remotamente, protegendo dados confidenciais e facilitando o trabalho remoto. Na esfera pessoal, os usuários de VPN podem contornar as restrições geográficas para acessar uma ampla gama de conteúdo, incluindo serviços de streaming ou sites de notícias bloqueados em certas regiões.

Além de melhorar a segurança e a privacidade, as VPNs também oferecem vantagens como proteção contra censura e mitigação de ataques cibernéticos. Em países com políticas estritas de censura da Internet, os cidadãos podem usar VPNs para acessar informações e se comunicar livremente, contornando as restrições impostas pelo governo.

Apesar de seus benefícios, é importante reconhecer que o uso de VPNs vem com seu próprio conjunto de desafios e limitações. A escolha de um serviço de VPN confiável é crucial, considerando que o provedor de VPN terá acesso aos dados do usuário, sublinhando a importância desta escolha. Portanto, os usuários devem considerar cuidadosamente questões como a política de privacidade e a jurisdição do provedor ao escolher um serviço VPN. Além disso, o uso de VPNs pode resultar em uma diminuição na velocidade da conexão devido à criptografia e à potencial distância física entre o usuário e o servidor VPN.

Em geral, as VPNs desempenham um papel fundamental na garantia da privacidade e segurança de dados na era digital, enfatizando sua importância. Sua capacidade de criptografar conexões e esconder a identidade do usuário torna-os uma ferramenta valiosa para indivíduos e organizações, fornecendo uma camada adicional de segurança em um ambiente online cada vez mais vulnerável a ameaças.

### RASPBERRY PI

O Raspberry Pi é um microcomputador de pequeno porte desenvolvido pela Fundação Raspberry Pi, uma organização educacional sem fins lucrativos. Lançado pela primeira vez em 2012, o dispositivo foi projetado para promover o ensino de ciência da computação básica em escolas e países em desenvolvimento. O Raspberry Pi ganhou ampla popularidade entre educadores, entusiastas de tecnologia, desenvolvedores e profissionais, que usam o dispositivo para uma variedade de projetos e aplicações.

Os modelos de Raspberry Pi variam em especificações técnicas, mas normalmente apresentam uma unidade central de processamento (CPU), RAM, portas USB, saída de vídeo HDMI, slot de cartão microSD (utilizado como armazenamento primário), conectividade Ethernet, e em alguns modelos, Wi-Fi e Bluetooth integrados. A versão mais recente, o Raspberry Pi 4, oferece desempenho significativamente melhorado com opções de até 8 GB de RAM, portas USB 3.0, suporte para monitores 4K duplos e um processador quad-core, melhorando suas capacidades para diversas aplicações.

Uma das principais vantagens do Raspberry Pi é a sua versatilidade, permitindo que ele seja usado em vários projetos que vão desde atividades educacionais até aplicações profissionais. Graças ao seu design aberto, uma grande quantidade de recursos e suporte da comunidade, o dispositivo pode ser usado em uma ampla gama de aplicações. No campo educacional, o Raspberry Pi é frequentemente empregado para ensinar programação e eletrônica, usando linguagens populares como Python e Scratch. Em projetos DIY (do-it-yourself), é comumente integrado em sistemas de automação doméstica, servidores de mídia, consoles de jogos retro e estações meteorológicas, entre outros.

Além disso, o Raspberry Pi tem sido uma ferramenta valiosa em áreas como a Internet das Coisas (IoT), onde serve como o núcleo de sistemas inteligentes e conectados, possibilitando aplicações e desenvolvimentos de IoT. Na pesquisa acadêmica e industrial, o dispositivo é usado para protótipos rápidos e o desenvolvimento de soluções inovadoras, graças ao seu baixo custo e facilidade de uso. A capacidade de executar sistemas operacionais baseados em Linux, como Raspberry Pi OS, Ubuntu e Windows 10 IoT Core, melhora ainda mais suas aplicações potenciais.

No entanto, apesar de suas inúmeras vantagens, o Raspberry Pi também tem limitações. O desempenho do dispositivo, embora notável pelo seu tamanho e custo, não é comparável ao de computadores tradicionais ou servidores dedicados. Além disso, a ausência de componentes como um disco rígido interno e a confiança no armazenamento de cartão microSD pode limitar a capacidade de armazenagem e velocidades de leitura/escritura.

O Raspberry Pi representa uma ferramenta revolucionária no campo da computação, oferecendo uma plataforma acessível e altamente adaptável para educação, desenvolvimento de projetos, pesquisa e inovação, revolucionando a forma como a tecnologia é utilizada em vários campos. A combinação de acessibilidade, expansibilidade e uma comunidade ativa de usuários e desenvolvedores torna o Raspberry Pi uma opção atraente para uma ampla gama de aplicações, desde educação básica até projetos avançados de IoT e protótipos industriais.

### PI-HOLE

Pi-hole é uma solução de bloqueio de anúncios e rastreamento de software que funciona como um servidor de rede local DNS (Domain Name System). Originalmente desenvolvido em 2014 por Jacob Salmela, o Pi-hole foi projetado para funcionar em dispositivos de baixo custo e de baixa potência, como o Raspberry Pi, embora também possa ser instalado em outras plataformas que suportam sistemas operacionais baseados em Linux.

O principal objetivo do Pi-hole é fornecer uma camada adicional de privacidade e segurança na rede, bloqueando automaticamente pedidos para domínios conhecidos por hospedar anúncios, rastreadores e conteúdo malicioso. Agindo como um servidor DNS local, o Pi-hole intercepta as solicitações de DNS de todos os dispositivos conectados à rede e verifica essas solicitações contra uma lista de blocos configurável. Se a solicitação corresponder a um domínio na lista de blocos, o Pi-hole impede que o dispositivo acesse esse domínio, impedindo assim o carregamento de anúncios e o rastreamento indesejado.

A vantagem significativa do Pi-hole reside na sua capacidade de bloquear anúncios e rastreadores em toda a rede, independentemente do dispositivo ou navegador. Isso inclui smartphones, tablets, Smart TVs e outros dispositivos conectados à rede local, proporcionando uma experiência de navegação mais limpa e mais segura sem a necessidade de instalar software adicional em cada dispositivo individual.

O Pi-hole oferece uma interface web intuitiva que permite aos usuários monitorizarem e gerenciar facilmente as solicitações de DNS e ajustar as listas de blocos conforme necessário. A interface também fornece estatísticas detalhadas sobre o tráfego de rede, incluindo o número de solicitações bloqueadas, os domínios mais acessados e os dispositivos mais ativos na rede. Além disso, os usuários podem adicionar entradas de white-list (lista branca) para garantir que certos domínios não sejam bloqueados, garantindo a funcionalidade de sites e serviços essenciais.

Em termos de segurança, o Pi-hole ajuda a proteger a rede contra ameaças cibernéticas, impedindo que dispositivos acessem sites maliciosos conhecidos. Isso pode reduzir o risco de ataques de phishing, malware e outras formas de ciberataques que dependem de domínios comprometidos para operar.

Além disso, o Pi-hole pode melhorar a segurança, integrando-se com outras soluções como VPNs (Virtual Private Networks) para fornecer uma proteção mais forte. Ao usar uma VPN em conjunto com o Pi-hole, os usuários podem criptografar seu tráfego na Internet, bloqueando anúncios e rastreadores, aumentando significativamente sua privacidade on-line.

O Pi-hole é uma ferramenta poderosa e versátil oferecem uma abordagem abrangente para bloqueio de anúncios e rastreamento em nível de rede. Sua capacidade de operar em dispositivos de baixo custo, como o Raspberry Pi, combinado com sua interface fácil de usar e funcionalidades robustas, torna-o uma solução atraente para os usuários que procuram melhorar a privacidade e segurança de suas redes. Pi-hole passa por atualizações contínuas para se adaptar aos novos métodos de publicidade e rastreamento, permitindo que os usuários fiquem proativamente à frente das ameaças online.

## Referencial teórico

Uma VPN (rede privada virtual) é uma tecnologia que estabelece uma conexão segura e criptografada através do roteamento de dados através da Internet pública, protegendo-os de intercepção e acesso não autorizado. Seu objetivo primordial é aumentar a segurança e a privacidade, substituindo o endereço IP do usuário pelo IP do servidor VPN, facilitando a navegação anônima e o acesso a conteúdo geograficamente restritos. As VPNs encontram ampla aplicação em ambientes corporativos para acesso remoto seguro e em cenários pessoais, oferecendo proteção contra censura e defesa contra-ataques cibernéticos.

O Raspberry Pi é um microcomputador compacto projetado para facilitar a instrução de ciência da computação. Devido à sua versatilidade e acessibilidade, o Raspberry Pi é empregado em uma variedade de projetos, que vão desde iniciativas educacionais até aplicações de IoT.

Pi-hole, uma solução para bloquear anúncios e rastreamento que funciona como um servidor DNS local, demonstra a utilização eficaz do Raspberry Pi. Ao bloquear pedidos para domínios maliciosos e anúncios em toda a rede, o Pi-hole melhora a privacidade e a segurança online, destacando sua integração eficaz com outras soluções, como VPNs, para proteção adicional.

### Citação indireta

A era digital trouxe consigo uma série de desafios de segurança. Todos os dispositivos conectados a uma rede estão sujeitos a riscos de segurança, incluindo downloads de malwares, acessos não autorizados e ataques de negação de serviço (DoS) que podem interromper serviços críticos e causar danos significativos aos sistemas (ISHAK et al., 2020).

Além disso, ataques Man-in-the-Middle (MITM) são uma ameaça significativa. Esses ataques permitem que invasores espionem, falsifiquem conteúdo e realizem roubo de identidade que juntamente a ferramentas de ataque sem fio, como scanners de rede, podem detectar redes vulneráveis e facilitar esses ataques (GOTO, 2019; AKRAM, SAEED, & DAUD, 2018).

A ISH Tecnologia, uma empresa nacional de segurança cibernética, lançou um relatório que aponta várias vulnerabilidades e ameaças digitais, incluindo o BlackByte ransomware e URLs maliciosos usados em cibercrimes. Estes endereços maliciosos podem ser escondidos em e-mails ou redirecionamentos de links, representando um risco significativo para os usuários que acidentalmente os acessam (CANALTECH, 2023).

As falhas de moderação em plataformas como Facebook, Instagram e YouTube também são uma preocupação. Elas facilitam a propagação de fraudes e anúncios enganosos, alcançando muitas vítimas potenciais. Um exemplo recente foi a exibição de um link patrocinado para uma página de vendas de bilhetes falsos para concertos da Taylor Swift nos resultados da pesquisa do Google, potencialmente levando a perdas financeiras ou roubo de informações pessoais (HELD, 2023).

Além disso, a geração de anúncios pode diminuir significativamente a experiência do usuário e a eficiência do dispositivo, levando a uma degradação do desempenho. Esses processos em segundo plano, gerados frequentemente sem o conhecimento do usuário, podem afetar significativamente a experiência do indivíduo e a eficiência do dispositivo (ABIDAH MAT TAIB et al., 2020).

A implementação de medidas como VPNs para navegar em redes Wi-fi públicas e o Pi-Hole para bloquear domínios com conteúdo malicioso oferecem uma solução econômica e eficaz para a proteção de dados (GONCHAROV et al., 2018), (XU & NI, 2020).

Portanto, a proteção contra tais ameaças é crucial para manter a integridade e a disponibilidade dos serviços online. A importância das ferramentas para gerir e minimizar estes impactos negativos é clara.

## Trabalhos correlatos

### “Securing Network Using Raspberry Pi by Implementing VPN, Pi-Hole, and IPS (VPiSec)”

O artigo "Securing Network Using Raspberry Pi by Implementing VPN, Pi-Hole, and IPS (VPiSec)" discute a implementação da segurança de rede usando um RaspBerry Pi, integrando três componentes cruciais: VPN, pi-hole, e IPS (Intrusion Prevention System). A VPN estabelece uma conexão segura entre dispositivos através de uma rede pública, criptografando o tráfego de dados e mascarando o endereço IP do usuário para proteger sua privacidade. No entanto, é importante notar que a VPN utilizada no projeto é a OpenVPN, que já não é recomendada pela Pi-Hole. O site da Pi-Hole afirma explicitamente: "OpenVPN não é mais recomendado." O texto continua a explicar que, embora o OpenVPN tenha sido eficaz no passado, é hora de migrar para soluções mais modernas e eficientes, como o WireGuard. Pi-Hole sugere que os usuários agora voltem sua atenção para o WireGuard, uma solução VPN avançada que oferece melhor desempenho, velocidades mais rápidas e implementação mais fácil.

No VPiSec, o Pi-Hole funciona como um servidor DNS local, melhorando a segurança da rede, bloqueando anúncios e rastreadores em toda a rede, e otimizando o desempenho, impedindo a recuperação de conteúdo indesejado. Enquanto isso, o IPS monitora a rede para atividades suspeitas, fornecendo detecção proativa e proteção em tempo real, embora possa apresentar falsos positivos e requerer conhecimentos técnicos para configuração e ajuste. Em conclusão, o VPiSec fornece um conjunto robusto de proteção de rede que exige configuração e manutenção meticulosas, especialmente à luz das sugestões revisadas do Pi-Hole sobre o uso de VPN.

### "SafeSearch: Obfuscated VPN Server using Raspberry Pi for Enhancing User Privacy".

O artigo "SafeSearch: Obfuscated VPN Server using Raspberry Pi for Enhancing User Privacy" explora a criação de um servidor VPN em um microcomputador RaspBerry Pi, destacando o uso do protocolo OpenVPN para este fim. Além disso, introduz a técnica de obstrução, que esconde o tráfego de VPN para se assemelhar aos dados da Internet regular, permitindo a evasão da inspeção profunda de pacotes para uma melhor proteção de privacidade. As vantagens deste sistema incluem maior privacidade e criptografia dos dados transmitidos através da VPN. No entanto, desafios como a velocidade de conexão potencial reduzida devido à criptografia e a complexidade de configurar e gerenciar a VPN devem ser considerados. Essencialmente, a utilização de um Raspberry Pi como um servidor VPN aumenta a proteção da privacidade, ao mesmo tempo que introduz obstáculos técnicos específicos, como a implementação de técnicas de obstrução para mascarar o tráfego VPN.

# MATERIAIS E MÉTODOS

### INSTALAÇÃO

Para realizar este trabalho, foi necessário reunir o hardware necessário, incluindo um Raspberry Pi 3 Model B, um cartão microSD de 16 GB, um cabo RJ-45 e uma fonte de alimentação. O microSD foi inserido no computador, e o site do Raspberry Pi foi acessado para baixar o aplicativo Raspberry Pi Imager. Em seguida, o Raspberry Pi Imager foi instalado no computador.

Com o aplicativo instalado, selecionou-se o sistema operacional desejado (neste caso, o Raspberry Pi OS Legacy 64-bit lite) e gravou-se no microSD usando o Raspberry Pi Imager como demonstrado na figura 1 – Raspberry Pi Imager.

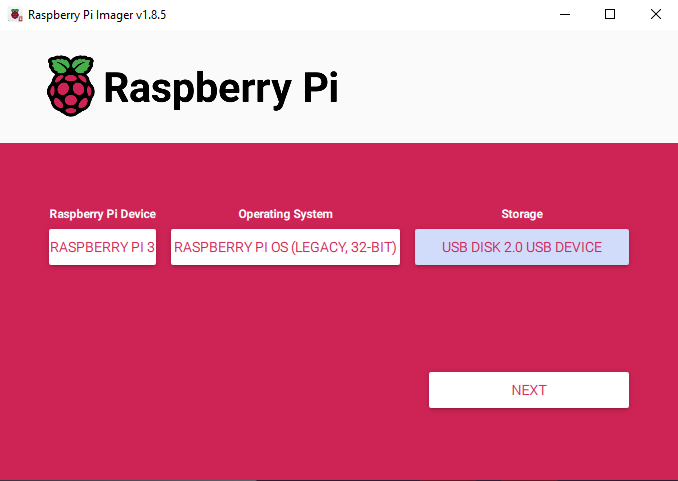


Figura - Raspberry Pi Imager

Na figura 1 apresenta a interface do Raspberry Pi Imager e nele necessitamos fazer algumas configurações e ajustes para poder acessar o Raspberry Pi via SSH, no "Raspberry Pi Device" selecionamos qual dispositivo iremos utilizar no caso do nosso projetos utilizamos um Raspberry Pi model 3B, na opção seguinte "Operating System"é a seleção do sistema operacional ou seja qual sistema queremos instalar no micro SD, no nosso uso utilizamos o sistema operacional Raspberry Pi OS Lite x64, esse sistema operacional não contém interface gráfica, na última opção "Storage" selecionamos em qual Cartão SD faremos a instalação, após a escolha do cartão selecionamos a opção "NEXT", nela contém uma importante configuração que é habilitar a função SSH para podermos conectar ao Raspberry Pi sem a necessidade de utilizarmos ele direto em um monitor.  
 As opções de SSH foram configuradas no Raspberry Pi Imager para permitir acesso remoto ao Raspberry Pi. O microSD foi então retirado do computador e inserido no Raspberry Pi, conectando-o ao roteador através do cabo RJ-45.

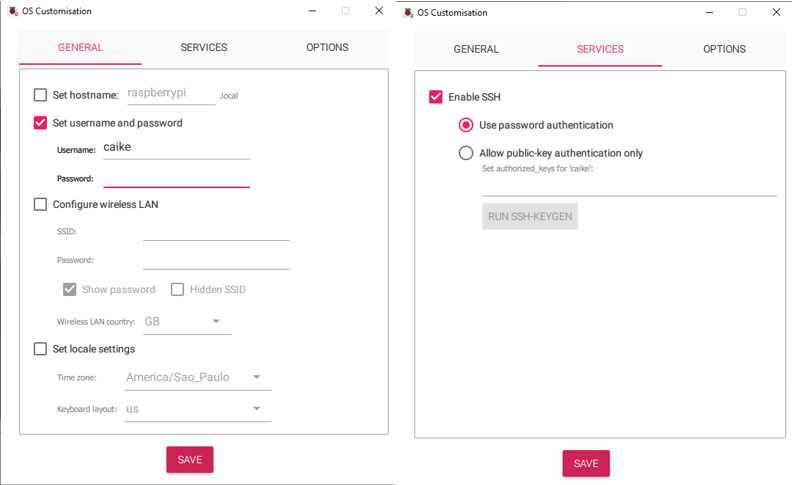


Figura - Customização do Sistema Operacional

Na figura 2 - Customização do Sistema Operacional, para habilitar função de SSH para conexão remota com o Raspberry Pi necessitamos entrar em "SERVICES" e a habilitar.

Conectou-se ao Raspberry Pi via SSH usando PowerShell ou um terminal, utilizando o IP atribuído ao Raspberry Pi na rede. Foram executados os comandos "sudo apt update" e "sudo apt upgrade" para atualizar o sistema operacional. Nas configurações do roteador, reservou-se um IP fixo para o Raspberry Pi, utilizando o endereço MAC e o IP do dispositivo.

No terminal, o Pi-hole foi baixado usando o comando "curl" com o URL do Pi-hole. Seguiram-se as instruções na tela para selecionar as opções desejadas, incluindo o servidor de upstream e a lista inicial de domínios bloqueados. Após a conclusão do download, anotou-se o IP atribuído ao Pi-hole, que seria utilizado para conectar-se localmente.

A interface gráfica do Pi-hole Admin foi acessada digitando o IP do Pi-hole seguido de "/admin" em um navegador web. Inseriu-se a senha solicitada para acessar o Pi-hole Admin. Na tela de administração do Pi-hole, foi possível acessar todas as informações da rede, incluindo domínios bloqueados, consultas realizadas e informações de hardware como uso da memória, temperatura e status do servidor.

Para adicionar uma lista de bloqueio, encontrou-se uma lista desejada na internet, copiou-se o URL do arquivo e colou-se na seção "Add Lists" no Pi-hole Admin. Após adicionar a lista, foi selecionada a opção de atualização na seção "Tools" para que o Pi-hole reconhecesse a nova lista de bloqueio. Com esses passos, foi possível configurar e utilizar o Pi-hole para melhorar a privacidade e segurança da rede.

# RESULTADOS

A implementação da combinação de VPN e Pi-hole utilizando um Raspberry Pi 3 Model B provou ser eficaz no bloqueio de anúncios e conteúdos indesejados.  
 Após a configuração do Pi-hole, houve uma redução significativa na quantidade de anúncios exibidos nos dispositivos conectados à rede. As estatísticas detalhadas fornecidas pela interface de administração do Pi-hole mostraram que muitas solicitações de DNS para domínios conhecidos por hospedar anúncios e rastreadores foram bloqueadas, resultando em uma navegação mais limpa e eficiente.

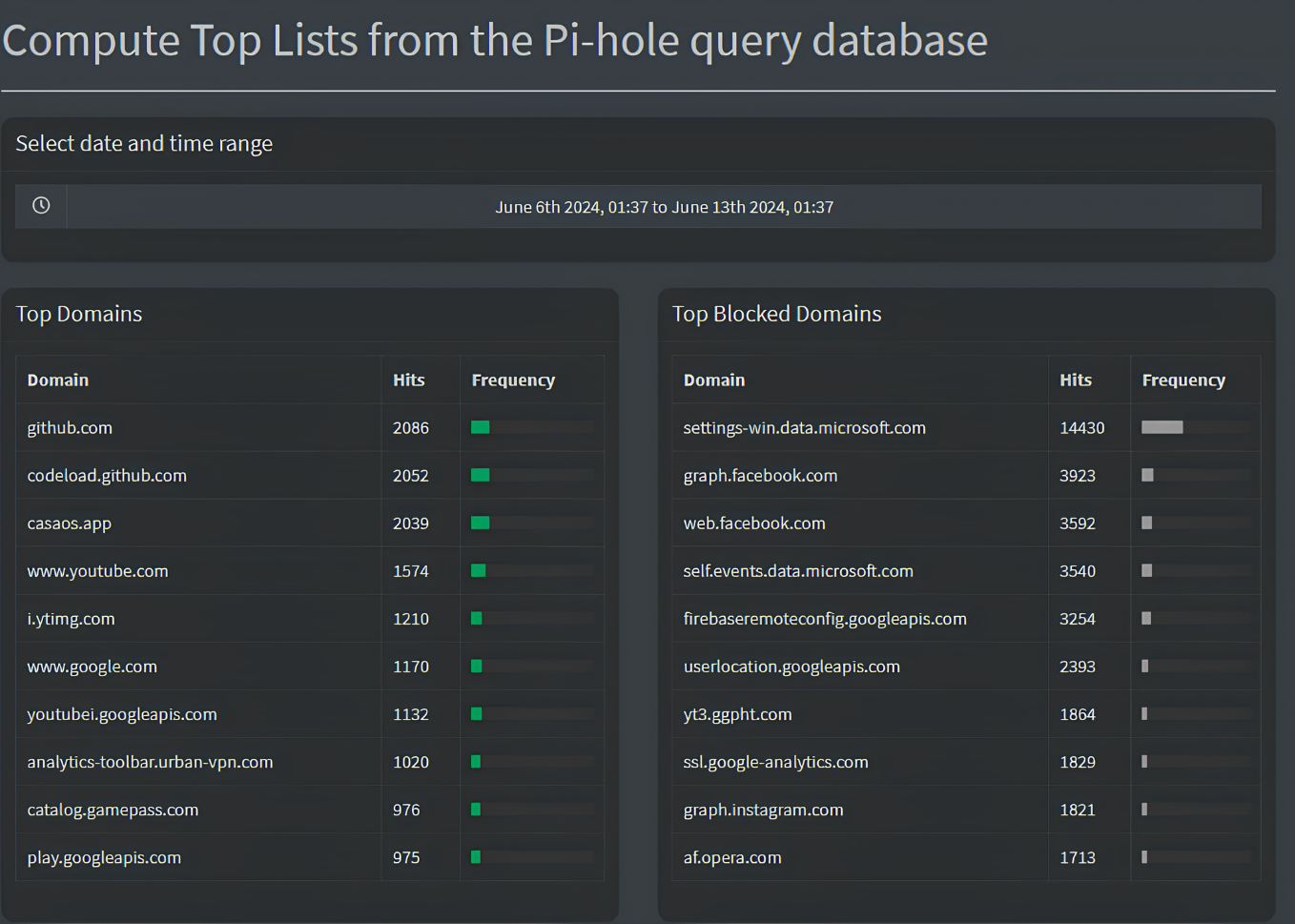


Figura - Últimos Sete dias de domínios bloqueados e permitidos

Na figura 3 - É possível identificar os domínios que foram mais permitidos e bloqueados dos últimos sete dias da rede nele é possível ver que o domínio que mais foi bloqueado é o settings.win.data.microsoft.com com a quantidade de 14430 bloqueios.

A privacidade dos usuários na rede foi significativamente aumentada pela integração do Pi-hole com uma VPN. A VPN criptografou o tráfego de dados, prevenindo a interceptação por terceiros, enquanto o Pi-hole bloqueou domínios associados a conteúdo malicioso. Essa combinação se mostrou eficaz na proteção contra-ataques de phishing, malware e outras ameaças cibernéticas.

O uso do Pi-hole para bloquear anúncios e rastreadores resultou em uma melhoria notável no desempenho da rede. Com menos conteúdo indesejado sendo carregado, a largura de banda foi utilizada de maneira mais eficiente, proporcionando tempos de carregamento de página mais rápidos e uma experiência de navegação mais fluida como mostrado na figura 4.

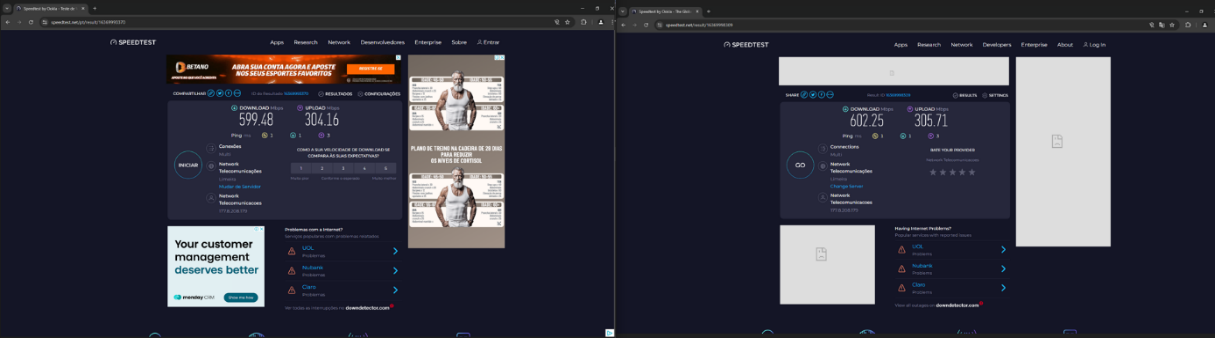


Figura - A direita Pi-hole desligado a esquerda Pi-hole ligado.

Figura 4 - Apresenta dois cenários um com o Pi-hole desligado imagem a esquerda, e com o Pi-Hole ligado imagem a direita, é possível verificar com o Pi-hole ligado a ausência de propaganda durante o teste de conexão de internet.

Por fim, a interface do Pi-hole forneceu estatísticas detalhadas sobre o tráfego de rede, incluindo o número de solicitações de DNS bloqueadas, os domínios mais acessados e os dispositivos mais ativos na rede. Essas informações foram valiosas para monitorar a atividade da rede e ajustar as configurações de bloqueio conforme necessário.

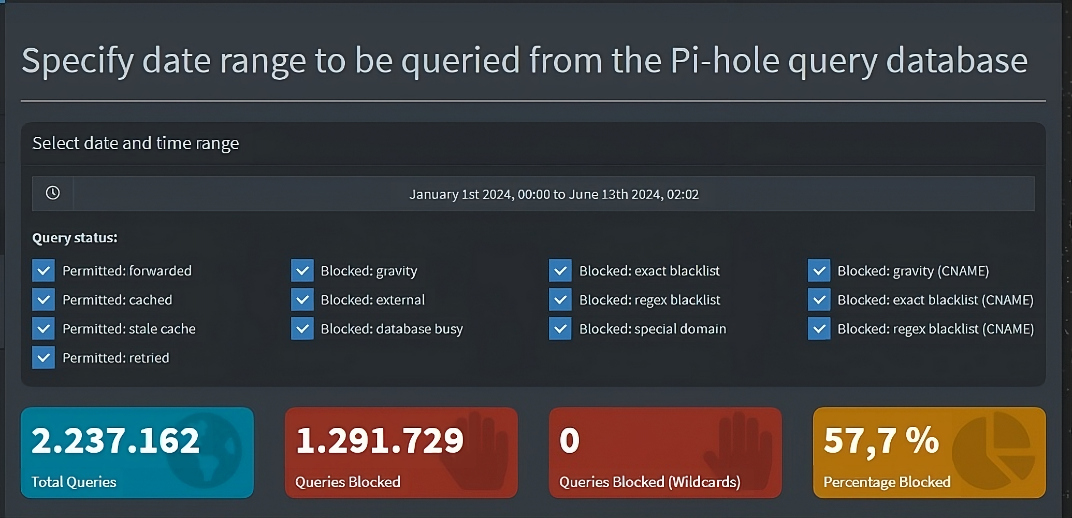


Figura - Total de queries do ano inteiro do Pi-Hole

Figura 5 – Total de queries do ano inteiro do Pi-Hole, puxa a quantidade total de solicitações desde o início do seu funcionamento trás de forma pratica a quantidade de solicitações 2.237.162, quantidade de solicitações que foram recusadas, 1.291.729 e o percentual em relação a quantidade de solicitação na rede inteira 57,7%, ou seja, de todas as solicitações que passaram pelo Pi-hole 57,7% foram bloqueadas.

# CONCLUSÃO

O trabalho teve como objetivo implementar uma solução de segurança e privacidade utilizando o Pi-hole em um Raspberry Pi Model 3 B+ em conjunto com uma VPN Tailscale. Através dessa configuração, buscou-se bloquear anúncios e rastreamentos indesejados a nível de rede, além de proporcionar uma conexão segura e privada para os dispositivos conectados. Ao longo do projeto, foi possível demonstrar que o uso combinado dessas tecnologias pode efetivamente melhorar a privacidade online e proteger a rede doméstica contra diversas ameaças cibernéticas.

Os objetivos do trabalho foram alcançados com sucesso. A configuração do Pi-hole mostrou-se eficaz no bloqueio de domínios indesejados, resultando em uma experiência de navegação mais limpa e segura. A integração com a VPN Tailscale adicionou uma camada adicional de segurança, garantindo que todo o tráfego de internet fosse criptografado e protegido contra interceptações. As ferramentas utilizadas proporcionaram uma solução robusta e acessível para usuários domésticos, comprovando a viabilidade de tais tecnologias em um ambiente de baixo custo e fácil implementação.

Durante a realização do trabalho, alguns desafios foram encontrados. A configuração inicial do Pi-hole e a integração com a VPN Tailscale exigiram um entendimento detalhado das redes e protocolos de internet, o que pode ser complexo para iniciantes. Além disso, houve a necessidade de ajustes finos nas listas de bloqueio do Pi-hole para evitar a interrupção de serviços legítimos, o que demandou tempo e paciência. No entanto, essas dificuldades foram superadas com pesquisa e experimentação contínuas, resultando em uma configuração estável e funcional.

O conhecimento aplicado neste projeto está diretamente relacionado as disciplinas do curso de Análise e Desenvolvimento de Sistemas sendo elas, Serviços e Infraestrutura de Redes, Criptografia e Cibersegurança e Arquiteturas de Computadores e Sistemas Operacionais. A compreensão dos conceitos de DNS, criptografia e tunelamento VPN foi fundamental para a implementação bem-sucedida do sistema. Além disso, a introdução ao dispositivo Raspberry Pi instigou a iniciativa para o projeto na área de IoT e segurança cibernética.

A implementação do Pi-hole em um Raspberry Pi Model 3 B+ com uma VPN Tailscale mostrou-se uma solução eficiente e acessível para melhorar a segurança e a privacidade da rede doméstica. Os resultados positivos alcançados evidenciam o potencial dessas tecnologias e abrem caminho para futuras melhorias e expansões para contextos domésticos.

## Trabalhos futuros

Uma direção promissora para o futuro envolve o uso de aprendizado de máquina para otimizar as listas de blocos do Pi-hole, permitindo ajustes adaptativos com base no comportamento do usuário. Usando algoritmos de aprendizagem de máquina, seria possível desenvolver um sistema que aprenda com o comportamento do usuário e ajuste automaticamente as listas de blocos para maximizar a eficiência e minimizar falsos positivos. Esta abordagem apresentaria uma experiência de navegação mais suave e segura, adaptando-se dinamicamente a ameaças emergentes e preferências do usuário.

Outra área para desenvolvimento adicional é a análise do desempenho e impacto da solução em redes maiores e ambientes corporativos. Este estudo pode avaliar a escalabilidade e eficácia do Pi-hole em ambientes com um maior número de dispositivos e tráfego de dados, e também a verificação da necessidade de hardwares mais robustos para suportar redes empresariais. Explorar a integração com firewalls de próxima geração e sistemas de detecção de intrusão (IDS) podem melhorar a postura geral de segurança e as capacidades de detecção de ameaças da rede.

Esses trabalhos futuros além de complementarem o conhecimento gerado por este estudo, contribuem para o avanço das práticas de segurança e privacidade em redes de computação, oferecendo soluções inovadoras e adaptáveis às necessidades emergentes da era digital.

# REFERÊNCIAS

ISHAK, Mohammad Fikri Hanif, Abidah Mat Taib et al. Securing network using Raspberry Pi by implementing VPN, Pi-Hole, and IPS (VPiSec) 2020. Disponível em: <https://doi.org/10.30534/ijatcse/2020/7291.32020>. Acesso em: 13 jun. 2024.

GOTO, H. Cityroam, providing secure public wireless LAN services with international roaming. In: Advances in Wireless and Optical Communications (RTUWO), 2018. Anais [...]. p. 204-208.

HELD, Darlan. Site falso vendia ingressos para shows da Taylor Swift no Brasil; veja como se proteger. G1, 21 jun. 2023. Disponível em: <https://g1.globo.com/tecnologia/noticia/2023/06/21/site-falso-vendia-ingressos-para-shows-da-taylor-swift-no-brasil-veja-como-se-proteger.ghtml>. Acesso em: 13 jun. 2024.

GONCHAROV, D. E.; ZARESHIN, S. V.; BULYCHEV, R. V.; SILNOV, D. S. Vulnerability analysis of the wifi spots using WPS by modified scanner Vistumbler. In: *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2018. *Anais* [...]. p. 48-51.

AKRAM, Z.; SAEED, M. A.; DAUD, M. Real time exploitation of security mechanisms of residential WLAN access points. In: International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 2018. Anais [...]. p. 1-5.

XU, Z.; NI, J. Research on network security of VPN technology. In: International Conference on Information Science and Education (ICISE-IE), 2020. Anais [...]. p. 539-542.