VPN - Ferramenta de Segurança Computacional

Gabriel Melo dos Santos[1], **Carlos Alberto da Silva**[2]

[1]Faculdade de Computação – Universidade Federal de Mato Grosso do Sul (UFMS)
Caixa Postal 549 – 91.501-970 – 79.070-900 – MS – Brazil

melo.gabriel@ufms.br, carlos.silva@ufms.br

Abstract. *This article aims to analyze security in public access networks obtained through the use of VPN connections. Bibliographic reviews and practical vulnerability tests were conducted to observe the security and privacy of data during network access with a VPN, evaluating aspects such as IP address protection, geolocation, open ports, data traffic, DNS and WebRTC leaks. The results of these tests showed a low occurrence of vulnerabilities and protected data traffic, demonstrating that VPN connections significantly contribute to the protection of user data while browsing on public access networks, guaranteeing greater privacy, anonymity, and data security. However, disadvantages include increased latency, network overload, and instability.*

Keywords. *cybersecurity; pentest; VPN.*

Resumo. *Este artigo visa analisar a segurança nas redes de acesso publicas obtidas através do emprego das conexões VPNs. Foram feitos revisões bibliográficas e testes práticos de vulnerabilidades, visando observar a segurança e a privacidade dos dados durante o acesso à rede com VPN, avaliando aspectos como a proteção de endereço IP, geolocalização, portas abertas, tráficos de dados, vazamentos de DNS e WebRTC. Evidenciou-se, nos resultados desses testes, a baixa ocorrência de vulnerabilidades e tráfegos de dados protegidos, demonstrando que as conexões VPN contribuem significativamente para proteção dos dados de usuário durante a navegação em redes de acesso público. Garantindo maior privacidade, anonimato e segurança dos dados. Contudo, como desvantagens, destacam-se o aumento da latência, a sobrecarga e a instabilidade da rede.*

Palavras-Chave. *cibersegurança; teste de penetração; VPN.*

1. Introdução

Com o avanço das tecnologias da informação e comunicação ampliou-se o uso de dispositivos digitais, como computadores, notebooks e smartphones, e seus aplicativos, tornando o acesso e o compartilhamento de informações mais ágil, rápido e interativo. No entanto, essa popularização também traz diversos desafios, como os *Fakes News*, o *bullying* digital, o vazamento de dados dentre outros, afetando a rotina das pessoas e organizações.

Juntamente com o fácil acesso à internet e à aquisição de dispositivos digitais observou-se o aumento da modalidade *Home Office*, sendo impulsionado na pandemia de Covid-19 em 2019, possibilitando que os funcionários realizassem suas funções com agilidade e segurança fora do ambiente da empresa [8].

Com a crescente disponibilização do acesso à internet por redes públicas em locais como clínicas, supermercados e órgãos públicos tem-se a questão da segurança dos dados, embora a maioria dessas redes exija autenticação, como usuário e senha, ou token, esse procedimento não garante segurança total, podendo expor usuários e organizações a ataques cibernéticos.

Observa-se que em diversas publicações acadêmicas apontam que a utilização do VPNs em *Home Office* contribui para reduzir riscos de ataques cibernéticos e garantir os princípios de

confidencialidade, integridade e disponibilidade da informação, promovendo segurança, eficiência na comunicação e proteção dos dados transmitidos [13].

Destaca-se a crescente oferta de serviços de proteção e segurança online, com opções gratuitas e pagas como a *Internet Security*. Esses serviços proporcionam navegação segura, oferecendo VPN para uso, conforme o cliente desejar, sendo recomendado na utilização de redes públicas [16].

Observa-se ainda que entre janeiro e setembro deste ano (2025), o Centro de Estudos de Resposta e Tratamento de Incidentes de Segurança no Brasil, registrou 340.933 notificações de incidentes, reforçando a necessidade da segurança dos dados [7].

Diante das preocupações com a segurança dos dados em redes públicas, surge o questionamento se o uso de VPN contribui na proteção dos usuário. Assim tem-se como objetivo analisar o nível de segurança proporcionado pelo uso de VPNs em redes públicas, descrevendo protocolos envolvidos, avaliando seus pontos positivos e negativos e realizando testes de vulnerabilidade com e sem o emprego da VPN.

Esta pesquisa apresenta uma revisão bibliográfica qualitativa sobre VPNs, abordando seus aspectos positivos e negativos. Em seguida, foram realizados testes práticos em rede pública empregando o Sistema Operacional (SO) *Windows* e utilizando as ferramentas *Nmap* [21] para detecção de portas e vulnerabilidades, *Wireshark* [5] para análise de tráfego, Meu IP [6] para verificar alterações de *Internet Protocol* (IP) e geolocalização, e *DNSLeakTest* [19] para identificar vazamentos de *Domain Name System* (DNS) e *Web Real-Time Communications* (WebRTC). Logo os dados coletados permitiram analisar o nível de segurança oferecido pelo uso de VPN, contribuindo para entender a eficácia desses protocolos na proteção das informações.

2. VPN - Virtual Private Network

Com a necessidade da troca de informações, como por exemplo matriz de uma empresa, suas filiais e seus funcionários, elas utilizavam diversos meios, como quadros de avisos, correio interno e externo, telefonia, fax e e-mail. No entanto, buscam constantemente melhorar a qualidade, eficiência, rapidez e segurança dessas comunicações, enfrentando altos custos com fornecimento e manutenção, especialmente ao utilizar linhas dedicadas para transmissão de dados.

Diante desses desafios e com o avanço do uso da Internet para troca de informações, impulsionado pela sua popularização e baixo custo, surgem novas tecnologias para otimizar processos e aumentar a segurança dos dados. Destacam-se protocolos como o *Hypertext Transfer Protocol* (HTTP) e soluções de conexão segura, como a *Virtual Private Network* (VPN), consideradas acessíveis.

Logo o VPN consiste em um serviço que estabelece, entre os dispositivos dos usuários e a *internet*, uma conexão virtual segura e criptografada para a transmissão e recebimento de dados entre os membros participantes da conexão estabelecida, conforme apresentado na Figura 1, assim assegurando a proteção dos dados e das atividades online.

Dessa forma, a VPN estabelece uma rede virtual, sem a necessidade de criar uma conexão física (linhas dedicadas), utilizando uma conexão de Internet entre os dispositivos participantes, logo os dados transmitidos entre os dispositivos são criptografados, de modo que apenas o dispositivo de destino possa descriptografar e ler a mensagem garantindo a segurança, e portando, a privacidade dos dados.

Diante do exposto em relação a VPN, nota-se um crescente aumento de sua utilização por empresas, organizações, acentuado pelo período pandêmico em virtude das atividades em *Home Office*, que requerem o acesso em sites ou sistemas da empresa numa rede pública (*Internet*) pelos seus funcionários, executando sua atividade laborais remotamente e compartilhando informações entre filiais e colegas de trabalho.

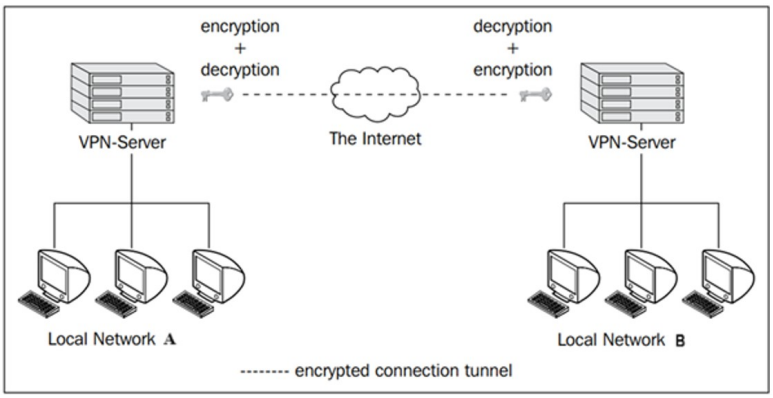

Figure 1. Exemplo de uma conexão VPN. [10]

2.1. Protocolos de VPN

Diversos protocolos foram desenvolvidos com objetivo de viabilizar a criação e emprego de VPNs. Os protocolos consistem em conjuntos de regras e procedimentos que determinam como os dados são protegidos e transmitidos entre dispositivos e servidores, especificando o modo de estabelecimento, autenticação, criptografia e transporte de dados na conexão de VPN.

Dentre os protocolos desenvolvidos destacamos o *Point-to-Point Tunneling Protocol* (PPTP), *Layer Two Forwarding* (L2F), *Layer Two Tunneling Protocol* (L2TP), *Layer 2 Security Protocol* (L2Sec), *Secure Socket Layer* (SSL), *IP Security Protocol* (IPSec) e *Open Source Virtual Private Network* (OpenVPN) [2, 10]. Porém, abordaremos os protocolos OpenVPN e o IPSec, por serem os mais utilizados em conexões da *internet*.

2.1.1. IPSec - IP Security Protocol

Sendo desenvolvido em 1995, o protocolo IPSec é reconhecido como um padrão de segurança para a camada 3 do modelo OSI pelo *Internet Engineering Task Force* (IETF). Composto por um conjunto de protocolos que oferecem serviços de integridade, autenticação, controle de acesso e confidencialidade, possibilitando interoperabilidade com diversos protocolos de diferentes camadas, como o *Transmission Control Protocol* (TCP), *User Datagram Protocol* (UDP) e *Internet Control Message Protocol* (ICMP) [10, 22], apresentado na Figura 2.

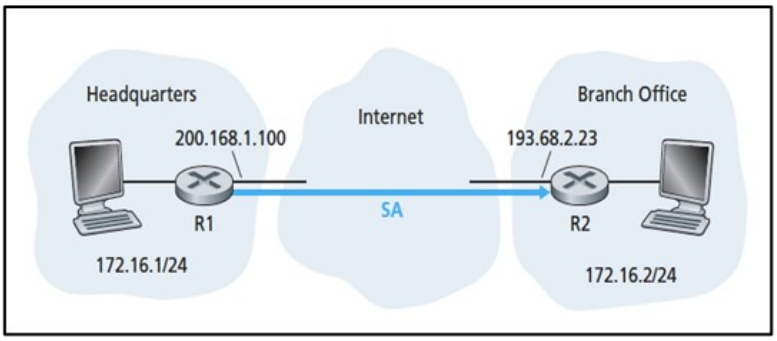

Figure 2. Exemplo do protocolo IPSec em uma conexão VPN [22]

O IPSec possui dois modos: transporte, que protege dados diretamente entre clientes com suporte ao protocolo, e túnel, que encapsula e criptografa pacotes entre *gateways*, usado quando os hosts não suportam IPSec. As principais características do IPSec são a *Authentication Header* (AH) para autenticação e prevenção de ataques, *Encapsulation Security Payload* (ESP) para confidencialidade por meio de criptografia, e gerenciamento de chaves, incluindo métodos de criação, distribuição, renovação e revogação, com destaque para o protocolo *Internet Key Exchange* (IKE) [2].

Dentre as principais vantagens do IPSec estão a segurança na camada de rede, transparência para aplicações (por atuar na camada 3 do modelo OSI) e ausência de impacto nas camadas superiores. O protocolo garante confidencialidade usando criptografia assimétrica e não requer aplicativos extras, dependendo apenas do suporte do sistema operacional para criar e gerenciar VPNs. Entre as principais desvantagens incluem a possibilidade de alteração inadvertida de privilégios ao acessar dispositivos via VPN, transferência de vulnerabilidades da rede para o ambiente corporativo, dificuldade de compatibilidade devido a padrões proprietários e firewalls, suporte limitado para multiprotocolo e *multicast* IP, alto consumo de processamento para criptografia e riscos adicionais por algoritmos com vulnerabilidades conhecidas.

2.1.2. OpenVPN - Open Source Virtual Private Network

Sendo desenvolvido por James Yonan em 2001, o OpenVPN é um protocolo de software livre de código aberto projetado para proporcionar altos níveis de segurança, apresentando integridade, autenticação, controle de acesso, confidencialidade, e a usabilidade, como consistência, acessibilidade e ainda a facilidade de uso. Ao longo do processo de comunicação esta conexão opera principalmente entre as camadas 2 e 3 do modelo *Open Systems Interconnection* (OSI), destacado na Figura 3 [10, 15].

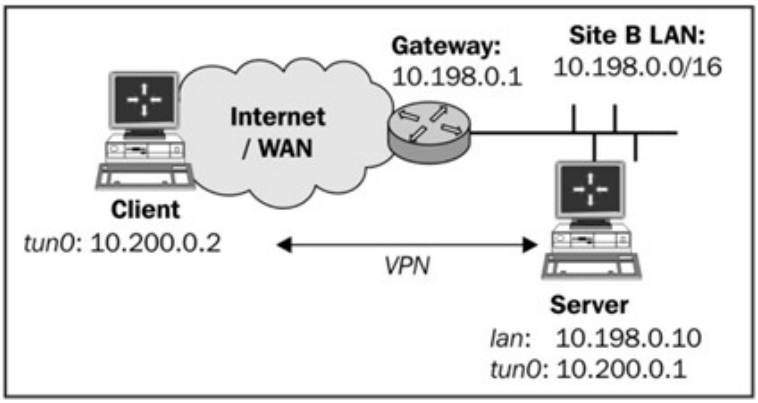

Figure 3. Exemplo do protocolo OpenVPN em uma conexão VPN [15]

O protocolo OpenVPN utiliza as interfaces *Universais Network TUNnel* (TUN) e *Network TAP* (TAP), ambas sendo projetos de código aberto suportados por sistemas operacionais como *Linux/Unix*, *Windows* e *Mac OS*. Essas interfaces possibilitam a emulação de dispositivos de rede onde a interface TUN opera na camada 3 enquanto a interface TAP atua na camada 2 do modelo OSI. Logo, podendo operar tanto no modo ponte, conectando redes distintas por meio da interface TAP como se fosse uma ponte física, quanto no modo roteado, em que as rotas são configuradas, por meio da interface TUN, para o parceiro VPN conectado [10].

O OpenVPN opera com interfaces TUN/TAP, o que torna sua arquitetura mais simples e elimina a necessidade de integração direta ao *kernel*. Compatível com sistemas como *Linux/Unix*, *Windows* e *Mac OS*, ele viabiliza conexões VPN entre diferentes plataformas, oferecendo suporte a diversos protocolos e portas (TCP/UDP) e, por ser software livre, possibilita adaptações conforme as demandas do usuário.

Dentre as principais vantagens do OpenVPN destacam-se a sua operação nas camadas 2 e 3 do modelo OSI, oferece flexibilidade com suporte a *proxy*, *firewall* e políticas específicas para túneis, permite o encapsulamento em diversos *firewalls* e *proxies*. Ainda temos a sua adaptabilidade ampliada pelo uso de *scripts* personalizados e sendo compatível com diversos dispositivos e sistemas operacionais. Por outro lado, temos complexidade de sua configuração, já que não possui interface gráfica nativa e depende da linha de comando e arquivos, podendo exigir softwares extras. Além disso, o consumo de recursos pode ser alto e seus túneis podem ser bloqueados por *firewalls*, dificultando a conexão e transmissão de dados.

3. Teste de Vulnerabilidade

Os testes de vulnerabilidades tem por objetivo identificar, analisar e propor meios de mitigar vulnerabilidades em dispositivos e em sistemas operacionais, consistindo em simulações de ataques realizadas com o uso de ferramentas e técnicas semelhantes às empregadas por invasores, como os testes de penetração (*Pentest*). Portanto, essas simulações permitem reproduzir cenários reais de possíveis ataques e invasões, contribuindo para a avaliação da segurança das redes e possibilitando a implementação de medidas preventivas [18].

Nos testes de vulnerabilidade serão aplicados o *Network Mapper* (Nmap) seguido da verificação de possíveis vazamentos de DNS, IP e WebRTC em um túnel VPN ativo, a análise do endereço IP, da localização geográfica, dos pacotes transmitidos e recebidos pelo túnel VPN, utilizando o Wireshark.

3.1. Nmap

O Nmap, desenvolvido por Gordon Lyon em 1997, sendo uma ferramenta amplamente empregada para varredura e exploração de redes. Este software utiliza pacotes IP para identificar dispositivos conectados à rede e analisar suas respectivas características [11].

Destaca-se que sendo um utilitário gratuito e de código aberto, compatível com os principais sistemas operacionais, o Nmap permite detalhar a disponibilidade de dispositivos na rede, os serviços oferecidos, os sistemas operacionais em execução, bem como a presença de filtros de pacotes ou firewalls, entre outras informações relevantes. Embora, seja projetado para realizar varreduras rápidas em grandes redes, o Nmap pode ser utilizado na análise de pequenas redes e dispositivos individuais [20].

Neste estudo, a ferramenta Nmap está sendo utilizada para verificar e identificar as possíveis portas abertas e os serviços em execução numa rede pública, logo contribuindo na detecção de vulnerabilidades associadas a essas portas. Os testes serão realizados em dois cenários distintos, sendo o primeiro sem o emprego do VPN, e o segundo com o emprego, permitindo uma comparação entre os níveis de exposição e proteção oferecidos.

3.2. Endereço IP e Localização

O IP foi desenvolvido no final da década de 1970 pela *Advanced Research Projects Agency Network* (ARPANET) com a finalidade de viabilizar o roteamento e endereçamento de pacotes de dados transmitidos por redes. O IP consiste em um conjunto de regras que orienta roteadores e dispositivos quanto à criação, identificação e envio de pacotes aos destinos designados [4].

Cada dispositivo ou domínio conectado à internet possui um endereço IP exclusivo. Assim ao enviar um pacote, o dispositivo remetente inclui as informações de IP de origem e de destino, esses pacotes são encaminhados entre roteadores até alcançar o dispositivo ou domínio final, conforme os dados presentes no cabeçalho do pacote [4].

Portando, serão utilizado o site Meu IP para verificar se ocorre alteração no endereço IP público e em sua geolocalização quando um serviço de VPN é ativado. Observa-se que a geolocalização, nesse contexto, refere-se ao mapeamento do endereço IP com o objetivo de identificar a localização geográfica real do dispositivo ou domínio conectado à internet. Este experimento visa observar se, ao ativar a VPN, o IP e sua localização deixam de refletir o provedor de internet original e passam a representar o servidor do provedor de VPN.

3.3. Vazamento de DNS e WebRTC

Criado por Paul Mockapetris em 1983, o DNS constitui um componente essencial da infraestrutura da *internet*, responsável pela tradução de nomes de domínio, como por exemplo a página *www.exemplo.com*, em endereços IP, como 124.87.9.200 (IPv4) ou 2001:db8:85a3::8a2e:370:7334 (IPv6). Portando é fundamental para que dispositivos e redes possam localizar e estabelecer

comunicação eficiente com servidores na internet, além de facilitar a memorização dos domínios pelos usuários. Assim, o DNS também viabiliza a conversão inversa, transformando endereços IP em nomes de domínio, recurso frequentemente utilizado em processos de diagnóstico e auditoria [3].

Já o projeto de código aberto WebRTC, desenvolvido em 2011 por uma ação de colaboração entre Google, Mozilla e Ericsson, e posteriormente padronizado pelo IETF e pelo *World Wide Web Consortium* (W3C), refere-se a uma tecnologia que possibilita que sites e aplicativos da web capturem e transmitam áudio e vídeo, além de permitirem a troca de dados diretamente entre navegadores, sem a necessidade de servidores intermediários, *plug-ins* ou softwares de terceiros. Essa solução permite o desenvolvimento de aplicações de comunicação em tempo real, como chamadas de vídeo, chats e transmissões ao vivo, utilizando apenas o navegador [9].

Assim no estudo, serão realizados testes de vazamento de DNS e de WebRTC com a utilização do site DNSLeakTest, sendo que o vazamento de DNS corresponde à situação em que, mesmo com a utilização de uma VPN, o dispositivo continua acessando os servidores DNS do provedor de internet, em vez de utilizar os servidores fornecidos pela VPN, o que pode resultar na exposição dos sites visitados. Logo, o vazamento de WebRTC acontece quando, ao utilizar uma VPN, o endereço IP real do dispositivo é revelado por meio da tecnologia WebRTC, comprometendo a anonimidade do usuário [12, 24].

3.4. Wireshark

Sendo desenvolvido em 1998 por Gerald Combs, o *Wireshark* (*Ethereal*) refere-se a uma ferramenta de código aberto para análise de pacotes, também conhecida como *sniffer* de rede. Possibilitando captura e registro do tráfego de dados em redes locais, facilitando o armazenamento dessas informações para análises posteriores. Com isso, torna-se viável identificar padrões de comunicação, falhas operacionais e potenciais vulnerabilidades na infraestrutura de rede [11].

A análise de pacotes consiste no processo de capturar e interpretar dados enquanto trafegam pela rede, com o objetivo de entender o que está ocorrendo com esses dados. Esse procedimento possibilita identificar as características da rede, os dispositivos conectados, determinar quais usuários ou aplicações utilizam a largura de banda disponível, podendo ainda analisar horários de maior uso, detectar possíveis atividades maliciosas e verificar a presença de aplicações vulneráveis ou sobrecarregadas [23].

Como disposto a ferramenta *Wireshark* será empregada para visualizar e compreender como os dados são protegidos em uma rede com VPN ativa. Além disso, será analisado o impacto da utilização da VPN sobre a velocidade de transmissão e o tempo de resposta da rede, permitindo avaliar possíveis variações no desempenho e na eficiência da comunicação.

4. Resultados dos testes vulnerabilidade

Os testes foram realizados em seis locais com acesso a *internet* com rede pública sendo elas duas clínicas de saúde (locais A e B), um supermercado (local C), duas farmácias (locais D e E) e uma instituição de ensino público (local F). Visto que devido a permanência, às vezes prolongada, seus frequentadores utilizam a rede pública para navegar nas mais diversas páginas, como mercados eletrônicos, bancos ou órgãos públicos dentre outros. Sendo utilizado para a geração da conexão VPN os serviços *Norton Secure VPN* [14] (*Wireguard* e OpenVPN) e o *Proton VPN* [1] (OpenVPN). Observa-se que os resultados apresentados não contêm os testes que não puderam ser realizados adequadamente pois esses testes (dos locais D, E e F) não permitiram a conexão por VPN.

Durante os testes com a utilização da ferramenta Nmap, foram realizados os escaneamentos das portas tanto do provedor de internet do local (sem a utilização do VPN) quanto do provedor de VPN na qual o dispositivo foi conectado, realizando o escaneamento nos IPs públicos dos mesmos provedores.

Sendo observado diferentes listas de portas abertas, desde lista sem nenhuma porta aberta até listas com diversas portas abertas mesmo com o VPN ativo, que aparentemente apresentam baixo risco de vulnerabilidade, já que conforme as configurações utilizadas na rede, podem bloquear todas as portas não essenciais ou deixar outras portas abertas para facilitar diversos tipos de serviços como serviço de telefonia virtual, o *Voice Over Internet Protocol* (VoIP). Na utilização do *Norton VPN*, observou-se que em um dos testes, havia duas portas abertas (443 e 8010) relacionadas ao protocolo *OpenVPN* (conforme a Figura 4), enquanto o *Proton VPN* apresentou um número maior de portas abertas nos testes realizados.

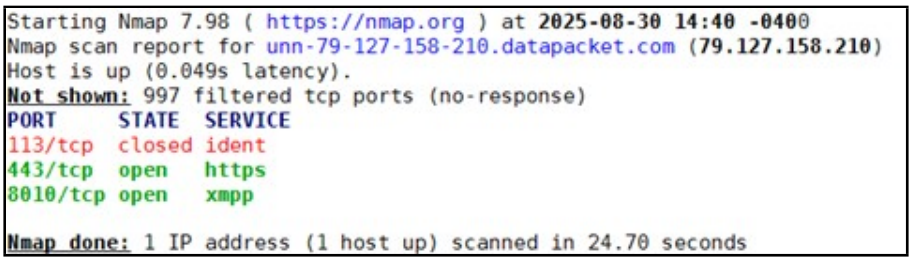

Figure 4. Teste do Nmap no local C utilizando o Norton VPN. Fonte: Autor (2025)

Durante a execução dos testes de IP e Localização empregando os serviços presente no site Meu IP, tanto o endereço IP quanto a geolocalização pública do dispositivo foram redirecionados para os do servidor do provedor de VPN, tanto no *Norton VPN* quanto no *Proton VPN*. Dessa forma, houve assim a alteração do IP (conforme apresentado na Figura 5) e da localização virtual utilizada pelo dispositivo para navegação na internet, refletindo os dados do servidor do provedor do VPN utilizado em vez do provedor de internet, reforçando assim a privacidade. Observa-se que o *Norton VPN* redirecionou o endereço IP para os servidores do Japão, já o Proton VPN redirecionou para os Estados Unidos.

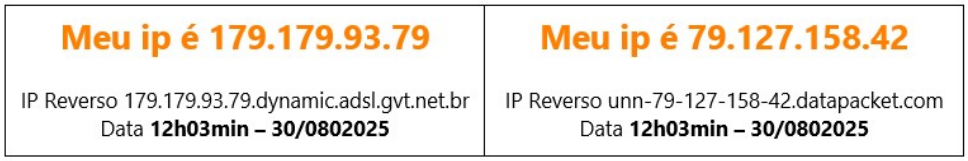

Figure 5. Mudança de endereço IP, sendo a esquerda sem o VPN e a direita com o VPN, no local A. Fonte: Autor (2025)

Nos testes de verificação de possíveis vazamentos de DNS e WebRTC utilizou-se os serviços presente no site *DNSLeakTest*, nas análises realizadas empregando os dois serviços de VPN citados, não sendo evidenciado a exposição do endereço IP público real do dispositivo, tampouco sinais de que os dados estejam sendo trafegados fora do túnel criptografado da VPN. Demonstrando que todo o tráfego está sendo corretamente roteado pela conexão VPN, impedindo que os servidores DNS do provedor de internet tenham acesso às requisições (conforme apresentado na Figura 6). Além disso, os testes confirmam que a API WebRTC não está capturando nem transmitindo o endereço IP público real do dispositivo, o que reforça a preservação da privacidade e a integridade da conexão.

Em relação aos testes realizados com o *Wireshark*, onde foi capturado e analisado todos os pacotes de dados transmitidos e recebidos durante a navegação de teste, sendo realizado por meio da navegação em oito sites, sendo considerado finalizado quando concluía-se o carregamento completo da página, a navegação de teste é composta pelos sites apresentados na Tabela 1. Os testes foram realizados em três condições distintas, sendo a primeira sem a utilização do VPN, a segunda com o *Norton VPN* e a terceira com o *Proton VPN*.

Com a execução do teste, constatou-se que, com a conexão VPN ativa, os pacotes de dados foram protegidos e criptografados por protocolos como *Wireguard* e *OpenVPN*, por meio dos protocolos *Secure Sockets Layer* (SSL), TCP e UDP, e que todo o tráfego era encapsulado no

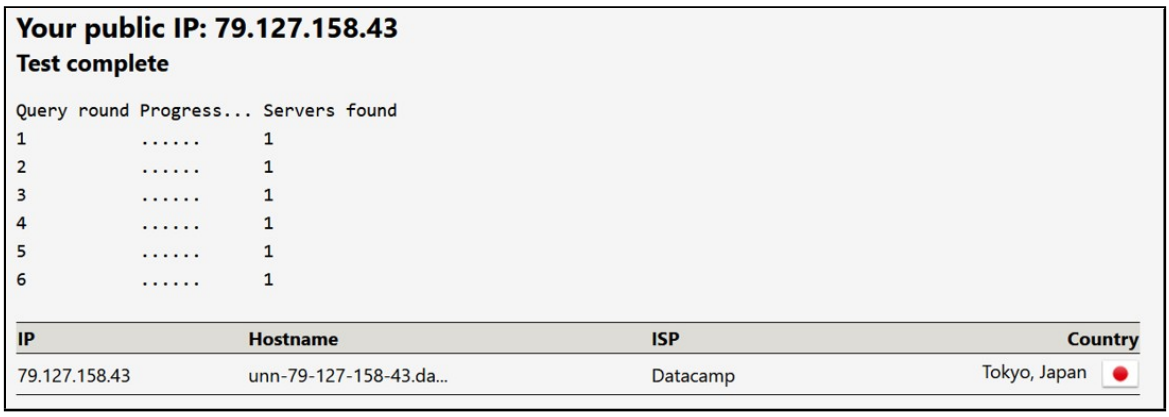

Figure 6. Teste de vazamento de DNS do local B. Fonte: Autor (2025)

Table 1. Lista de sites utilizado no teste de navegação do Wireshark. Fonte: Autor (2025)

— Site	Endereço —
— Institucional 1	https://www.gov.br/pt-br —
— Institucional 2	https://meususdigital.saude.gov.br/ —
— Bancário 1	https://www.bb.com.br/site/ —
— Bancário 2	https://www.sicredi.com.br/home/ —
— Comércio Eletrônico 1	https://www.kabum.com.br/ —
— Comércio Eletrônico 2	https://www.mercadolivre.com.br/ —
— Comércio Eletrônico 3	https://www.amazon.com.br/ —
— Formulário Online	https://docs.google.com/forms/u/0/ —

túnel VPN, proporcionando maior segurança e anonimidade das informações transmitidas conforme demostrado na Figura 7.

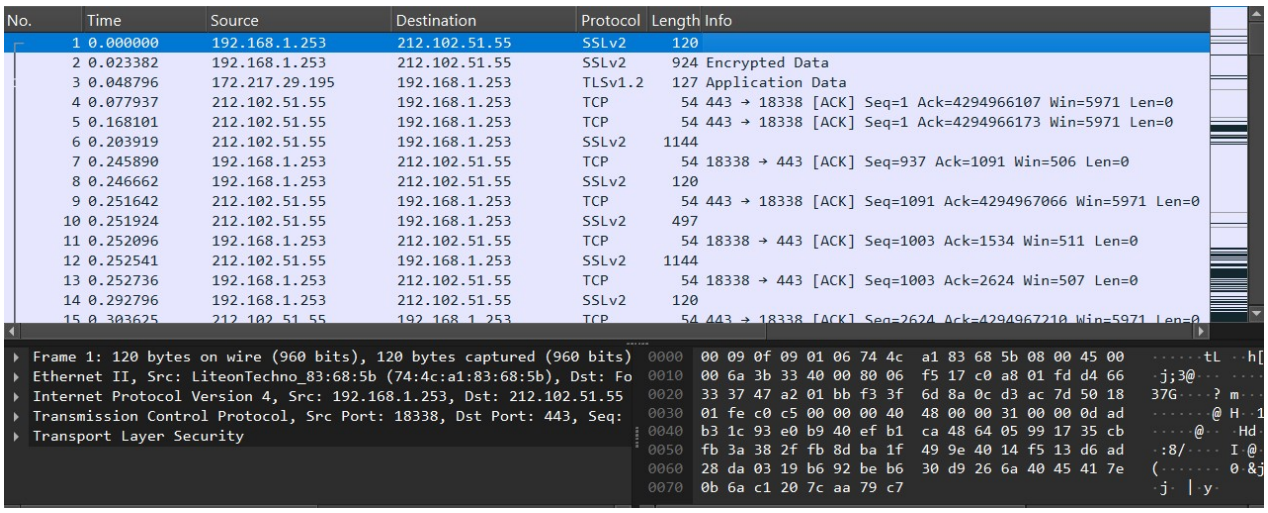

Figure 7. Teste de tráfico de dados no *Wireshark* do local C. Fonte: Autor (2025)

Além disso, observou-se que o túnel VPN apresentou poucos indícios de comportamentos suspeitos, como recebimento de dados inesperados ou envio de informações para servidores não autorizados conforme o que foi configurado a conexão VPN. Evidenciando a eficácia da VPN na proteção das comunicações em rede, destacando, contudo, a necessidade de realizar o monitoramento contínuo para assegurar a integridade e a segurança dos dados trafegados.

Também observou-se como esperado um tempo maior para a navegação na internet quando utiliza-se uma conexão VPN conforme apresentado na Figura 8 que compara os tempos de duração dos testes em cada rede (local A, B e C).

Observa-se na Figura 8, que os tempos de navegação nas redes de acesso públicas apresenta-se

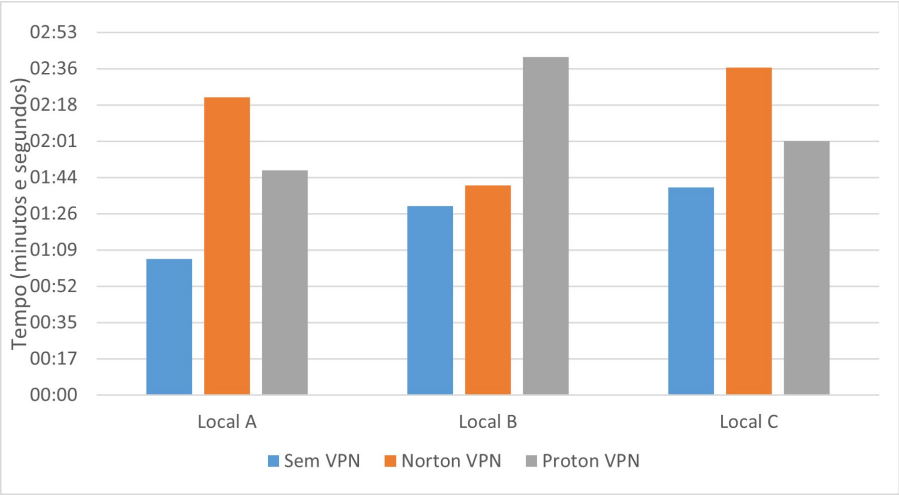

Figure 8. Gráfico de tempo de duração do teste Wireshark. Fonte: Autor (2025)

pouca diferença entre os tempos dos provedores de VPN utilizados, porém, observa-se ainda que os tempos relativamente altos se comparados aos tempos sem utilização do VPN, logo temos uma navegação mais lenta que pode desestimular o seu emprego pelo usuário. Ainda destaca-se que o tempo para o carregamento das páginas depende além do VPN, também o número de usuários conectados simultaneamente, quantidade de tráfico que a rede suporta e a qualidade do sinal do roteamento.

5. Conclusões e Trabalhos futuros

Nos três locais com rede de acesso público em que não foi possível estabelecer conexão VPN, é provável que o bloqueio tenha ocorrido devido à ação do firewall ou ao fechamento das portas necessárias para a VPN, impedindo a conexão [17].

Nos locais com rede pública em que a VPN foi conectada com sucesso, verificou-se que ela mascara o IP e assegura anonimato e privacidade. A maioria das portas permanece fechada, e as abertas se relacionam ao protocolo e serviços do provedor de VPN. Durante a navegação nas páginas testadas, os dados estavam protegidos e criptografados, sem indícios de vazamentos de DNS ou WebRTC, nem comportamentos suspeitos. Os testes indicam que a VPN oferece maior privacidade, anonimato e segurança, mas pode causar aumento no tempo de navegação, sobrecarga e possíveis instabilidades na rede.

Muitos usuários de redes públicas não usam ou desconhecem o serviço de VPN, seja gratuito ou pago, espera-se que estas informações possam incentivar a utilização da VPN em redes de acesso públicas e mitigar riscos de acesso indevidos aos dados. Como possibilidade de trabalhos futuros, destaca-se a análise do uso de VPN em dispositivos móveis, especialmente Android, além de ações para divulgar esse serviço à população.

References

[1] Proton AG. Proton vpn. `https://protonvpn.com/pt-br`, 2025.

[2] Fábio Borges, Bruno Alves Fagundes, and Gerson Nunes Da Cunha. *VPN: Protocolos e Segurança*. PhD thesis, Laboratório Nacional de Computação Científica - LNCC, 9 2007.

[3] Chrystal R. China and Michael Goodwin. O que é dns (domain name system)? `https://www.ibm.com/br-pt/think/topics/dns`, 4 2024.

[4] Cloudflare. O que é ip? `https://www.cloudflare.com/pt-br/learning/network-layer/internet-protocol/`, 2025.

[5] Gerald Combs. Wireshark. `https://www.wireshark.org/`, 2025.

[6] Datahouse. Meuip. https://meuip.com.br/, 2025.

[7] Núcleo de Informação e Coordenação do Ponto BR. Cert.br - estatística de incidentes notificados ao cert.br. https://stats.cert.br/incidentes/, 2 2025.

[8] Marcelo Renato do Carmo Pereira Filho and Matheus Carvalho Leal. A importancia da vpn (virtual private network) durante a pandemia covid-19: Uma revisao de literatura. *JNT-FACIT BUSINESS AND TECHNOLOGY JOURNAL*, 1:314–332, 2021.

[9] MDN Web Docs. Webrtc api. https://developer.mozilla.org/pt-BR/docs/Web/API/WebRTC_API, 2025.

[10] Markus. Feilner and Norbert. Graf. *Beginning OpenVPN 2. 0. 9 : Build and integrate Virtual Private Networks using OpenVPN*. Packt Publishing, Limited, 12 2009.

[11] Douglas Martins Ferreira. *Análise de pentest como ferramenta para segurança da informação*. PhD thesis, Pontifícia Universidade Católica de Goiás - PUC Goiás, 12 2024.

[12] GeeksforGeeks. What is dns leak? https://www.geeksforgeeks.org/computer-networks/what-is-dns-leak/, 7 2025.

[13] Alexandre Guimarães. *Proposta de um modelo de segurança para VPNs na interligação de redes corporativas*. PhD thesis, Universidade Federal de Pernambuco - UFPE, 2 2004.

[14] Gen Digital Inc. Norton 360 premium - norton vpn. https://br.norton.com/, 2025.

[15] Jan Just Keijser. *OpenVPN Cookbook - Second Edition*. Packt Publishing, Limited, second edition edition, 2 2017.

[16] Kaspersky Lab. O que é uma vpn? como funciona, tipos e benefícios das vpns. https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn, 2025.

[17] Kaspersky Lab. Por que a vpn não conecta? como corrigir problemas na vpn. https://www.kaspersky.com.br/resource-center/preemptive-safety/common-vpn-problems, 2025.

[18] Alexandre Lepesqueur and Italo Oliveira. *Pentest, Análise e Mitigação de Vulnerabilidades*. PhD thesis, Universidade de Brasília, 2 2012.

[19] IVPN Limited. Dns leak test. https://dnsleaktest.com/, 2025.

[20] Gordon Lyon. *Nmap Network Scanning - The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com, 12.2.2008 edition, 1 2009.

[21] Gordon Lyon. Nmap: the network mapper. https://nmap.org/, 2025.

[22] Nicolas Menezes, Túlio Porto, and Victor Hugo Ferreira. Ipsec - 2019-1. https://www.gta.ufrj.br/ensino/eel878/redes1-2019-1/vf/ipsec/, 2019.

[23] Chris Sanders. *Análise de pacotes na prática: Usando Wireshark para solucionar problemas de rede do mundo real*. Novatec Editora Ltda, 3° edição edition, 6 2017.

[24] Surfshark. Vazamento de webrtc: como testar e evitar vazamentos de ip. https://surfshark.com/pt-br/webrtc-leak-test, 2025.