UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS QUIXADÁ

CURSO DE GRADUAÇÃO EM REDES DE COMPUTADORES

DANILO ALVES BARBOSA

ANALISANDO A QUALIDADE DE SERVIÇO EM VIDEOCHAMADAS SOB TUNELAMENTO VPN: UMA COMPARAÇÃO ENTRE OPENVPN E WIREGUARD

QUIXADÁ

2026

DANILO ALVES BARBOSA

ANALISANDO A QUALIDADE DE SERVIÇO EM VIDEOCHAMADAS SOB TUNELAMENTO VPN: UMA COMPARAÇÃO ENTRE OPENVPN E WIREGUARD

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Redes de Computadores do Campus Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de tecnólogo em Redes de Computadores.

Orientador: Prof. Dr. João Marcelo Uchôa de Alencar.

QUIXADÁ

2026

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

B196a Barbosa, Danilo Alves.
Analisando a qualidade de serviço em videochamadas sob tunelamento VPN: uma comparação entre OpenVPN e WireGuard / Danilo Alves Barbosa. – 2026.
44 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Redes de Computadores, Quixadá, 2026.
Orientação: Prof. Dr. João Marcelo Uchôa de Alencar.

1. VPN. 2. Qualidade de Serviço (QoS). 3. OpenVPN. 4. WireGuard. 5. Desempenho de Rede. I. Título.
CDD 004.6

DANILO ALVES BARBOSA

ANALISANDO A QUALIDADE DE SERVIÇO EM VIDEOCHAMADAS SOB TUNELAMENTO VPN: UMA COMPARAÇÃO ENTRE OPENVPN E WIREGUARD

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Redes de Computadores do Campus Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de tecnólogo em Redes de Computadores.

Aprovada em: 22/01/2026.

BANCA EXAMINADORA

Prof. Dr. João Marcelo Uchôa de Alencar (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Arthur de Castro Callado
Universidade Federal do Ceará (UFC)

Prof. Dr. Michel Sales Bonfim
Universidade Federal do Ceará (UFC)

À minha família, pelo suporte contínuo durante essa longa caminhada.

AGRADECIMENTOS

A Deus pelo dom da vida, pela saúde da minha família e pela capacidade de adquirir novos conhecimentos.

Aos meus pais, Lucimar e Luciano, pelo amor incondicional e pelo incentivo para continuar seguindo em frente, mesmo diante de tantos obstáculos. Sem vocês esta realização não seria possível.

À minha irmã mais velha, Lucélia, pelas revisões nas fases iniciais e ao meu primo, Renan, pelas reflexões críticas a respeito da escrita.

Ao Prof. Dr. João Marcelo Uchôa de Alencar, pela excelente orientação.

Aos professores participantes da banca examinadora Prof. Dr. Arthur de Castro Callado e Prof. Dr. Michel Sales Bonfim pelo tempo, pelas valiosas colaborações e sugestões.

À Instituição e todos que de alguma forma contribuíram para o meu crescimento acadêmico e como pessoa.

Muito obrigado.

"'Cause you only live forever in the lights you make"– The Kids from yesterday.

(My Chemical Romance)

RESUMO

O crescente aumento na adoção de VPNs por empresas e usuários comuns evidencia a preocupação com a segurança da informação. Apesar das vantagens oferecidas, as VPNs podem causar impactos negativos na entrega da qualidade de serviço e da qualidade de experiência de aplicações em tempo real, como é o caso das videochamadas. Por meio de experimentos em ambientes controlados, este trabalho se propôs a quantificar o impacto causado pelo uso de duas soluções VPN distintas, OpenVPN e WireGuard, em videochamadas. Ao final do experimento, foi possível concluir que ambas as soluções VPN se mostraram estáveis e capazes de entregar um elevado índice de qualidade de serviço e de experiência.

Palavras-chave: VPN; Qualidade de Serviço (QoS); OpenVPN; WireGuard; Desempenho de Rede.

ABSTRACT

The growing increase in the adoption of VPNs by companies and individual users highlights concerns about information security. Despite the advantages offered, VPNs can cause negative impacts on the delivery of quality of service and quality of experience for real-time applications, such as video calls. Through experiments conducted in controlled environments, this study aimed to quantify the impact caused by the use of two distinct VPN solutions, OpenVPN and WireGuard, in video calls. At the end of the experiment, it was possible to conclude that both VPN solutions proved to be stable and capable of delivering a high level of quality of service and quality of experience.

Keywords: VPN; Quality of Service (QoS); OpenVPN; WireGuard; Network Performance.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

EAD	Ensino a Distância
QoE	Qualidade de Experiência
QoS	Qualidade de Serviço
RTP	*Real-time Transport Protocol*
TIPHON	*Telecommunications and Internet Protocol Harmonization Over Networks*
VoIP	*Voice over Internet Protocol*
VPN	*Virtual Private Networks*

SUMÁRIO

1 INTRODUÇÃO

A partir do ano de 2020, com a ascensão da educação e trabalho à distância, o mundo observou de perto a crescente tendência de pessoas que de alguma forma estudam ou trabalham à distância. Os chamados Ensino a Distância (EAD) e *home office* (trabalho remoto) são duas modalidades relativamente novas, tendo ganhado mais notoriedade durante a pandemia do COVID-19, iniciada em 2019, cujos impactos se estenderam até 2023. Segundo Rani *et al.* (2021), esse contexto contribuiu significativamente para a ampliação dessas modalidades. Em ambas, é possível notar que a comunicação é um fator crucial para o bom funcionamento dessas atividades, por isso as instituições de ensino e empresas começaram a recorrer às chamadas videoconferências, que usam a *Internet* para transmitir voz e vídeo, criando assim um ambiente onde vários usuários podem engajar em suas aulas, reuniões ou mesmo conversas casuais entre usuários comuns, que também fazem uso desse serviço. Um exemplo disso foi a plataforma da *Google*, o *Google Meet*, que é uma plataforma de videoconferências, e teve um aumento expressivo na quantidade de usuários durante esse período. É possível verificar em Schaevitz (2020) os resultados divulgados de forma oficial pela própria Google.

Ainda nesse contexto, é válido destacar que embora essas plataformas possuam mecanismos de segurança próprios, como uso de contas exclusivas para acesso e um sistema de *whitelist*, onde apenas usuários previamente adicionados podem conectar-se, é possível notar que ainda existe a possibilidade de que ocorram vazamentos de dados ou interceptação do tráfego durante a rota na rede. Isso ocorre principalmente em redes públicas como aeroportos, restaurantes e locais públicos, ou mesmo a residência do usuário. Buscando solucionar essas questões, as empresas começaram a adotar o uso das chamadas *Virtual Private Networks* (VPN), que criam uma conexão segura e criptografada entre determinados pontos da rede, prevenindo assim o vazamento ou interceptação das comunicações por terceiros, mesmo em redes públicas e potencialmente inseguras, efetivamente adicionando mais uma camada de segurança, como mostra a pesquisa de Chacon *et al.* (2006).

Outro uso recorrente de VPN está relacionado aos usuários que buscam driblar bloqueios de certos conteúdos em uma determinada localização geográfica. Nesse contexto, a VPN atua mascarando o endereço IP e a localização real do usuário, pois ela criptografa o tráfego e o envia para o servidor VPN, que este então realiza a ponte entre o usuário e o serviço requisitado, o que leva esse serviço a validar que o usuário está acessando o conteúdo de dentro da área geográfica na qual o servidor VPN se encontra. De acordo com Aceto *et al.* (2015), isso

ocorre principalmente em plataformas de *streaming* de vídeo, como o *YouTube* ou *Netflix*, que limitam o acesso a certos conteúdos por não possuírem localização no idioma daquele país por exemplo.

Apesar das vantagens oferecidas, as VPNs apresentam algumas limitações e desvantagens inerentes ao seu funcionamento, que impactam o usuário e que devem ser consideradas. Como já referido, as VPNs utilizam-se de criptografia para manter o tráfego confidencial, o que pode ocasionar lentidão, pois o tráfego precisa passar por mais etapas de processamento antes de chegar ao destino. Além disso, geralmente o tráfego precisa percorrer um caminho geograficamente maior, saindo primeiro do cliente, passando pelo servidor VPN até chegar no serviço requisitado, e depois fazer o caminho inverso. Entre essas etapas é preciso considerar que o tráfego passará por mais nós da rede (roteadores) do que o normal, o que contribui para o atraso. Nesse contexto, o atraso da rede causa impactos negativos principalmente às aplicações sensíveis a latência, como é o caso das videochamadas descritas anteriormente, o que pode ser sentido pelo usuário na forma de travamentos ou perda de conexão, piorando assim sua experiência com o serviço (Chacon *et al.*, 2006).

Diante desse cenário, manifestam-se múltiplas soluções VPN, tais como o GRE+IPSec e L2TP+IPsec, que serão abordadas de forma detalhada adiante neste estudo, porém aqui é válido ressaltar que ambas apresentam complexidades de configuração e integração limitada. Em contraponto, surgem alternativas mais flexíveis, que se integram em diferentes sistemas operacionais, e possuem maior liberdade de configuração como é o caso do OpenVPN[1], consolidado desde 2001, e que será objeto de estudo desse trabalho. Como já referido, o OpenVPN é amplamente utilizado, e diante disso surgem outras opções dessa categoria, como é o caso do WireGuard[2], que segundo o site oficial da ferramenta, é mais moderno e propõe-se a ser mais simples de configurar e oferecer melhor desempenho do que o OpenVPN, devido ao seu código simples e algoritmo de criptografia mais eficiente.

Dadas as particularidades de cada abordagem, este trabalho abordará uma comparação de desempenho direta, sem a influência da rede entre duas soluções : OpenVPN e WireGuard, tendo como foco o seu desempenho em videochamadas. Visando isso, serão realizados experimentos em um ambiente controlado, onde serão coletadas as métricas críticas para o bom funcionamento desse tipo de aplicação.

[1] openvpn.net
[2] wireguard.com

1.1 Objetivos

1.1.1 Objetivo geral

Realizar uma análise comparativa de desempenho das ferramentas OpenVPN e WireGuard, com ênfase na avaliação da Qualidade de Serviço (QoS) em aplicações sensíveis à latência, especificamente videoconferências.

1.1.2 Objetivos específicos

- Prover uma comparação atual, oferecendo uma base de resultados sólida para ajudar na tomada de decisão sobre qual ferramenta usar.
- Caracterizar as ferramentas OpenVPN e WireGuard, descrevendo suas arquiteturas, propostas e quais algoritmos usam.
- Analisar a influência das VPNs na experiência percebida pelo usuário.
- Propor recomendações de uso dos protocolos.

2 FUNDAMENTAÇÃO TEÓRICA

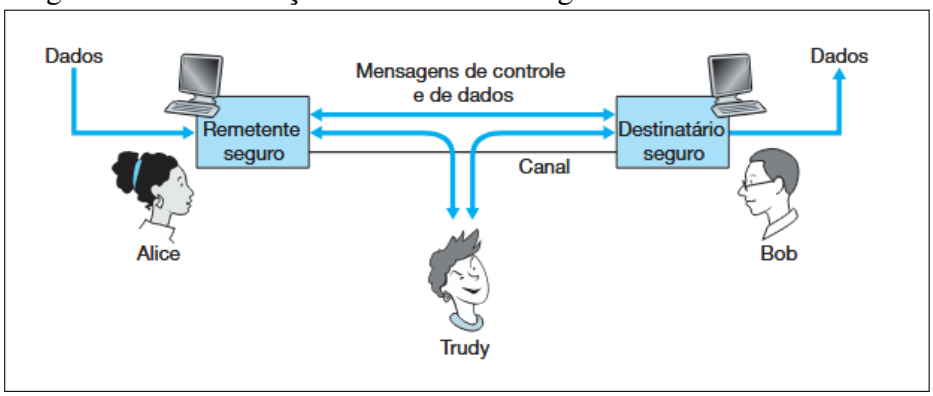
Neste capítulo serão abordados os principais conceitos relacionados às VPNs bem como suas aplicações mais comuns, além dos benefícios e impactos previstos em videochamadas. A exposição dos fundamentos visa oferecer embasamento para a compreensão das tecnologias envolvidas, suas arquiteturas, protocolos e aplicações no contexto analisado.

2.1 Criptografia

Segundo Kurose e Ross (2021), no contexto da *Internet* a criptografia pode ser definida como a ciência de proteger dados por meio de algoritmos criptográficos. Ao utilizar chaves, esses algoritmos transformam uma informação clara em algo que pareça ilegível para pessoas não autorizadas, ou seja, aquelas que não possuem acesso à chave utilizada pelo algoritmo para realizar a criptografia dos dados. Dessa forma, quem não detém a chave empregada no processo de criptografia não consegue acessar as informações transmitidas. As VPNs usam esse meio para tornar a comunicação entre as duas partes confidencial, dificultando assim que um intruso consiga obter a informação clara que está sendo transmitida.

Para entendermos melhor como funciona a criptografia na prática, imagine a seguinte situação: Duas pessoas (Bob e Alice) buscam comunicar-se de forma confidencial diante de um meio inseguro. Para isso, eles concordam em trocar suas mensagens de forma criptografada, pois há um ouvinte não autorizado entre eles (Trudy). Em um meio inseguro, Trudy pode ler claramente as mensagens que Bob e Alice estão trocando, assim como ilustrado na Figura 1.

Figura 1 – Comunicação em um meio inseguro

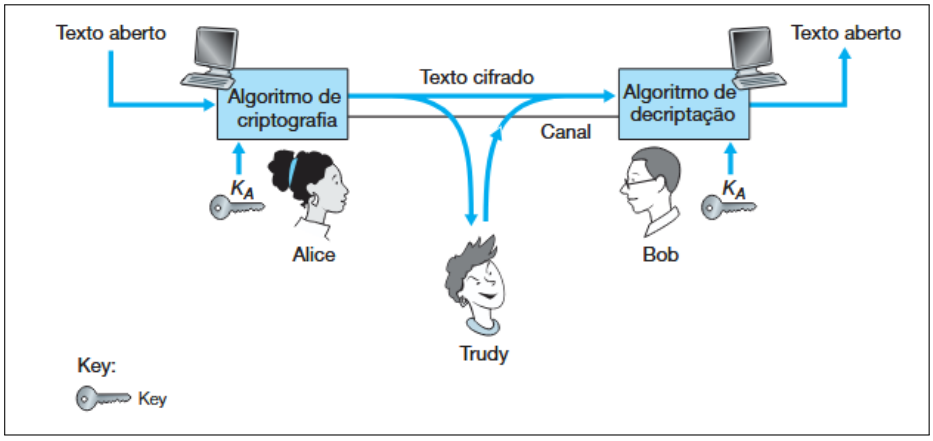


Fonte: Adaptado de (Kurose; Ross, 2021).

Atualmente os algoritmos de criptografia podem ser divididos em duas categorias: algoritmos de criptografia simétrica e assimétrica. Na criptografia simétrica, ambas as partes

utilizam a mesma chave para criptografar e descriptografar uma mensagem. Esse tipo de algoritmo é considerado seguro, desde que ambas as partes consigam manter a chave confidencial e o algoritmo possua elevada complexidade. A criptografia simétrica oferece maior velocidade por ser mais leve, requerendo menos recursos computacionais para executar seus processos. A Figura 2 ilustra uma troca de mensagem usando algoritmo de criptografia simétrica. Os símbolos K_A representam a mesma chave compartilhada.

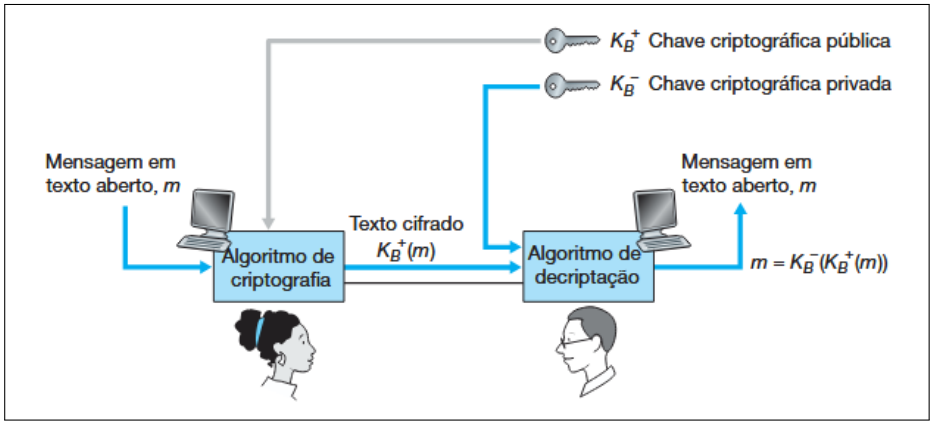
Figura 2 – Comunicação em um meio inseguro usando criptografia simétrica



Fonte: Adaptado de (Kurose; Ross, 2021).

Os algoritmos de criptografia assimétrica usam duas chaves: Uma chave pública para cifrar os dados, que pode ser distribuída livremente, e uma chave privada para descriptografar os dados, onde esta última não deve ser compartilhada. Ambas as partes possuem o seu próprio par de chaves, na analogia, Alice usa a chave pública de Bob para criptografar a mensagem, depois envia o texto cifrado para Bob. Para ser capaz de ler a mensagem, Bob usa sua chave privada para descriptografar os dados enviados por Alice. No envio de uma mensagem para Alice, Bob realiza o mesmo processo, agora com a chave pública de Alice para criptografar, e Alice usa sua chave privada para descriptografar e ler o texto. Esse tipo de algoritmo apresenta elevada segurança, pois é computacionalmente inviável descobrir o texto claro tendo apenas acesso à chave pública, entretanto esse meio é consideravelmente mais lento do que a criptografia simétrica, dado que o algoritmo apresenta elevado uso de recursos computacionais. A Figura 3 ilustra uma troca de mensagens usando criptografia assimétrica.

Figura 3 – Comunicação em um meio inseguro usando criptografia assimétrica



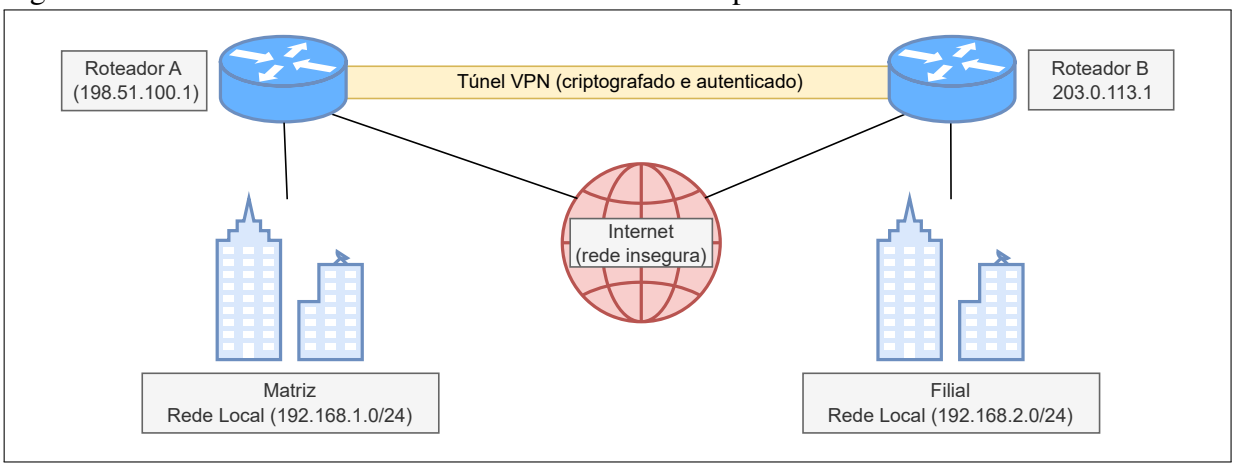
Fonte: Adaptado de (Kurose; Ross, 2021).

2.2 *Virtual Private Networks (VPN)*

Para entendermos o funcionamento de uma VPN, precisamos ter como ponto de partida a definição de rede privada. As redes privadas consistem de um grupo de dispositivos que estão conectados entre si, porém isolados da *Internet*, geralmente por um *firewall*, onde essencialmente, todo o tráfego de *Internet* precisa passar por um grande filtro antes que possa entrar ou sair daquela rede (Kurose; Ross, 2021). Esse tipo de arquitetura é muito comum em ambientes corporativos, onde vários usuários estão conectados na rede da instituição, que em muitos casos possui aplicações locais, tais como servidores de *e-mails* corporativos, servidores de arquivo e periféricos

VPN é uma rede privada criada sobre a infraestrutura de rede pública (*Internet*). Os pacotes são encapsulados em outros pacotes com cabeçalhos adicionais, criando assim um túnel virtual que permite o roteamento entre as duas redes privadas, similar a como se estivessem conectadas diretamente por meios físicos. Para garantir a segurança dos pacotes durante o percurso na rede, os protocolos de tunelamento VPN adicionam criptografia nos pacotes encapsulados, garantindo assim a confidencialidade e a autenticidade das informações transmitidas (Stallings, 2021). A Figura 4 ilustra o funcionamento do túnel VPN conectando dois escritórios fisicamente distantes de uma corporação em uma só rede privada.

Figura 4 – Funcionamento do túnel VPN sobre uma rede pública



Fonte: Elaborada pelo autor.

2.3 Principais arquiteturas VPN

De acordo com Budiyanto e Gunawan (2023), as VPNs podem ser classificadas em dois tipos de arquitetura. A *Remote Access* VPN e a *Site-to-Site* VPN. No meio corporativo ambas desempenham papéis diferentes, porém o princípio de funcionamento continua sendo o mesmo.

2.3.1 A arquitetura Remote Access VPN

Em muitos casos, por questões de segurança, muitos dos recursos e aplicações utilizados pelos trabalhadores de uma companhia só podem ser acessados localmente, como é o caso dos servidores de arquivo FTP e aplicações internas. O propósito dessa arquitetura é possibilitar que um usuário remoto acesse a rede interna da companhia, tornando assim possível acessar os recursos já mencionados de forma segura, mesmo em redes públicas e inseguras. Os protocolos mais comuns nessa categoria são: OpenVPN, IKEv2/IPSec, L2TP/IPSec e SSTP.

2.3.2 A arquitetura Site-to-Site

A arquitetura Site-to-Site tem como objetivo conectar duas redes privadas, algo muito comum no meio corporativo. Os protocolos mais comuns nessa categoria são o IPSec e GRE+IPSec. O GRE funciona adicionando cabeçalhos sobrepostos a diversos tipos de pacotes, incluindo os pacotes usados por videochamadas (SIP, H.323, WebRTC e RTP). Embora o GRE possibilite criar redes privadas virtuais, ele não oferece a segurança que a criptografia proporciona, em virtude disso, esse protocolo é comumente combinado com o IPsec, que adiciona criptografia

sobre os pacotes transmitidos, proporcionando assim confidencialidade sobre o tráfego.

2.3.2.1 A arquitetura Cloud VPN

A arquitetura *Cloud* VPN, pode ser vista como uma arquitetura *Site-to-Site*, porém não requer o uso de equipamentos ou infraestruturas no local. O servidor VPN é hospedado na nuvem, os escritórios filiais conseguem conectar-se por meio do túnel VPN criado por esse servidor. Os protocolos mais comuns nessa categoria são: IPSec, IKEv2, SSL e OpenVPN. Esta categoria em específico, apresenta maiores vantagens por serem altamente escaláveis e de fácil manutenção, pois como já referido, não necessitam de servidores físicos. Alguns provedores que fornecem esse serviço são a AWS (com o AWS VPN), Google Cloud (Cloud VPN), ou Azure (Azure VPN Gateway).

2.4 Impactos do uso de VPN na Qualidade de Serviço (QoS) e Qualidade de Experiência (QoE) em videochamadas

Apesar das vantagens oferecidas, as VPNs apresentam desvantagens inerentes ao seu funcionamento. A criptografia e a sobreposição dos pacotes resultam em maior tempo de processamento pela rede durante o percurso fim-a-fim do tráfego (Stallings, 2021). Segundo Kurose e Ross (2021), aplicações como videochamadas e serviços de *Voice over Internet Protocol* (VoIP) utilizam o protocolo de rede *Real-time Transport Protocol* (RTP) para o transporte eficiente de dados em tempo real, como áudio e vídeo. Essas aplicações são as que mais sofrem com encargos do tráfego de rede.

2.4.1 Qualidade de Serviço (QoS)

Segundo Kurose e Ross (2021) a Qualidade de Serviço pode ser descrita como um conjunto de tecnologias e técnicas que garantem o bom funcionamento de aplicações críticas sensíveis à latência. As videochamadas e *streaming* de vídeo necessitam de uma alta taxa de *bits* e baixa latência para operar corretamente. As métricas de rede que representam esses parâmetros são descritas em:

– *Delay e Interarrival*: O *delay* (latência) corresponde ao tempo total em que uma requisição leva para ser completamente processada. O processo inclui o envio da requisição pelo cliente, o percurso e processamento da rede, o processamento pelo servidor e o retorno da

resposta até o cliente. Cada uma dessas etapas contribui para o *delay* geral da transmissão. No contexto das VPNs esse processo é geralmente mais demorado, pois a requisição do cliente percorre um caminho mais longo na rede. A medição do atraso absoluto requer protocolos específicos e sincronização absolutamente precisa dos relógios do emissor e receptor, que em ambientes reais não ocorre com frequência. A solução proposta foi usar o *interarrival*, que é o tempo de chegada entre dois pacotes RTP consecutivos no receptor, que embora não represente o atraso fim-a-fim, faz com que seja possível evidenciar o atraso experienciado pelo tráfego durante seu percurso na rede.

- *Jitter*: O *jitter* é a variação do atraso entre pacotes consecutivos. Essa flutuação reflete na instabilidade da rede.
- *Packet loss*: O *packet loss* (perda de pacotes) ocorre quando um pacote, seja ele requisição ou resposta, é descartado em algum ponto da rede. Isso ocorre em razão do roteamento ineficiente, congestionamento na rede ou mesmo por problemas no meio físico. Os pacotes VPN possuem um tamanho maior, contribuindo para a demora no processamento e ineficiência de roteamento, o que pode levar a uma taxa maior de perda.
- *Throughput*: O *throughput* (vazão) é a quantidade real de dados que a rede ou sistema consegue transportar. No contexto das videochamadas, essa métrica está relacionada com quantas videochamadas simultâneas a rede ou sistema consegue suportar.
- *Bitrate*: O bitrate é a taxa de geração de dados do reprodutor de vídeo. No contexto desse trabalho, essa métrica atua como complementar ao *throughput*, a proximidade dessas métricas indica que a demanda está sendo atendida pela rede.

A análise dessas métricas pode ajudar a identificar possíveis problemas ou gargalos na rede, no contexto desse trabalho, tais métricas ajudam a dimensionar o impacto que cada solução VPN causa na fluidez do tráfego na rede.

2.4.2 Qualidade de Experiência (QoE)

Segundo Tanenbaum *et al.* (2021), a Qualidade de Experiência (QoE) pode ser descrita como o quão satisfeito está o usuário final durante e após o uso do serviço. No contexto das chamadas de vídeo, a Qualidade de Experiência é regida pela fluidez na reprodução da voz e vídeo, e a qualidade em que o vídeo está sendo reproduzido. Tendo isso em vista, durante o experimento será coletada a seguinte métrica de QoE em cada cenário:

- *Playback continuity*: Representa a fluidez durante a reprodução da mídia. Em videochama-

das, uma fluidez constante é essencial para um bom entendimento da mensagem que está sendo transmitida entre os usuários.

Para garantir uma experiência satisfatória em videochamadas ao usuário final, a métrica mencionada precisa exibir desempenho aceitável, caso contrário o usuário pode perceber travamentos na voz e vídeo durante a sua sessão.

2.5 Soluções VPN em estudo

Essa seção tem como objetivo contextualizar as soluções VPN abordadas como objeto de estudo deste trabalho, OpenVPN e WireGuard, destacando os aspectos que diferem de soluções VPN tradicionais, tais como as já mencionadas GRE+IPSec, L2TP+IPsec.

2.5.1 OpenVPN

Criado em 2001 e atualmente já consolidado no mercado, o OpenVPN é uma ferramenta de código aberto que facilita a criação de túneis VPN de ambas as arquiteturas *Site-to-Site* e *Remote Access*, pois não depende de manipulação avançada de *hardware* e sistema operacional, diferindo-se dos protocolos convencionais. Tendo em vista sua facilidade de uso, a configuração por meio de arquivos de texto pode ser realizada por administradores de rede e usuários. O OpenVPN integra-se com facilidade em diversos sistemas operacionais tais como Windows, Linux, Mac, iOS e Android (OpenVPN Technologies, Inc., 2025).

Diferentemente da maioria das soluções VPN já mencionadas, o OpenVPN consegue operar mesmo em ambientes de rede que possuem *firewalls* e NAT, sendo assim uma escolha sólida para ambos usuários comuns e corporações. O OpenVPN pode operar sobre os protocolos da camada de transporte TCP ou UDP. No Quadro 1 estão dispostos os algoritmos de criptografia mais comuns usados por esta solução.

Quadro 1 – Algoritmos de criptografia comumente usados no OpenVPN

Categoria	Algoritmo	Tipo de criptografia	Observações
Autenticação (TLS)	RSA-2048 / RSA-4096	Assimétrica	Compatível e seguro
Autenticação (TLS)	ECDSA (ex: P-256)	Assimétrica	Mais leve e rápido
Autenticação (TLS)	Ed25519	Assimétrica	Moderno e eficiente
Troca de chaves	Diffie-Hellman (DH)	Assimétrica	Tradicional, mais pesado
Troca de chaves	ECDH (ex: Curve25519)	Assimétrica	Leve e seguro
Criptografia de dados	AES-256-CBC	Simétrica	Popular, precisa HMAC
Criptografia de dados	AES-128/256-GCM	Simétrica	Modo AEAD, eficiente
Criptografia de dados	ChaCha20-Poly1305	Simétrica	A partir da versão 2.4 (2016)
Integridade (HMAC)	HMAC-SHA1	Simétrica (MAC)	Antigo, para compatibilidade
Integridade (HMAC)	HMAC-SHA256	Simétrica (MAC)	Atual padrão recomendado
Integridade (HMAC)	HMAC-SHA512	Simétrica (MAC)	Uso para alta segurança

Fonte: Elaborado pelo autor, baseado em (OpenVPN Technologies, Inc., 2025).

2.5.2 WireGuard

Para fazer frente ao OpenVPN, em 2016 surgiu o WireGuard, com a proposta de ser mais leve do que o seu competidor. Além de manter a simplicidade na configuração e possuir integração com os mesmos sistemas operacionais que o OpenVPN, o WireGuard foi criado visando oferecer um melhor desempenho geral, isso se deve ao seu código fonte ser mais simples e ao uso de algoritmos criptográficos mais eficientes por padrão, como é o caso do ChaCha20 e o Ed25519. O WireGuard opera exclusivamente sobre o protocolo de transporte UDP, e assim como o OpenVPN, também pode ser usado em ambientes de rede que operam com *firewall* ou NAT (WireGuard Development Team, 2025). No Quadro 2 estão dispostos os algoritmos de criptografia que o WireGuard suporta.

Quadro 2 – Algoritmos de criptografia suportados pelo WireGuard

Categoria	Algoritmo	Tipo de criptografia	Observações
Autenticação / Assinatura	Ed25519	Assimétrica	Assinatura de chaves públicas
Troca de chaves	Curve25519 (ECDH)	Assimétrica	Estabelecimento de segredo
Criptografia de dados	ChaCha20	Simétrica	Cifra rápida e segura
Integridade	Poly1305	Simétrica (MAC)	Autenticação de mensagens
Hash / KDF	BLAKE2s	Simétrica (hash)	Função hash rápida e segura

Fonte: Elaborado pelo autor, baseado em (WireGuard Development Team, 2025).

3 TRABALHOS RELACIONADOS

Este capítulo é dedicado a apresentar trabalhos que abordam um estudo similar a este, com o objetivo de oferecer uma base de comparação e validar os resultados desta pesquisa, seja usando métricas ou abordagens semelhantes. Serão descritas as abordagens, métricas e objetos de estudo escolhidos por seus autores, bem como os resultados obtidos ao final dos experimentos.

3.1 *Analysis of Streaming Video on VPN Networks Between OpenVPN and L2TP/IPSec*

O trabalho de Wahanani *et al.* (2021), documenta uma avaliação comparativa de desempenho entre os protocolos de tunelamento VPN OpenVPN e L2TP/IPSec, com foco em QoS relacionado ao *streaming* de vídeo. Para tal, os autores criaram um ambiente de testes simulado consistindo em computadores clientes, dois servidores, sendo um servidor de *streaming* de vídeo e o outro, um servidor VPN, além de três roteadores atuando como elos da rede entre os clientes e servidores.

Para medir a Qualidade de Serviço, os autores coletaram métricas de *throughput*, *delay*, *jitter* e *packet loss*. O experimento consistiu em capturar os pacotes da rede VPN usando a ferramenta Wireshark nas máquinas cliente, enquanto realizavam o acesso do vídeo transmitido por *streaming*. Além disso, foram realizados testes com diferentes resoluções de vídeo, as quais foram mencionadas: 360p, 480p e 720p.

Ao fim do experimento, concluiu-se que o protocolo de tunelamento VPN OpenVPN mostrou-se superior ao L2TP/IPSec nas métricas de *throughput*, *delay* e *packet loss*, perdendo apenas no quesito de *jitter*. Concluiu-se que o OpenVPN apresenta melhor desempenho geral no que se refere a *streaming* de vídeo, sendo assim a escolha mais sólida diante do cenário apresentado.

A abordagem desta pesquisa é inspirada no trabalho descrito de Wahanani *et al.* (2021), entretanto esta pesquisa difere nos objetos de estudo e tipo de experimento realizado, como pode ser observado no Quadro 3.

Quadro 3 – Comparativo técnicas e objetos de estudo

Trabalho	Tipo de experimento	Objetos de estudo
Wahanani *et al.* (2021)	Simulação	L2TP/IPSec e OpenVPN
Esta pesquisa	Emulação e virtualização	OpenVPN e WireGuard

Fonte: Elaborado pelo autor.

3.2 *Performance Evaluation of Multimedia over MPLS VPN and IPSec Networks*

O trabalho de Sllame (2022) avalia o desempenho dos protocolos MPLS VPN e IPSec com foco em tráfego FTP, HTTP, VoIP e videoconferências. Usando uma ferramenta de simulação de redes OPNET, o autor criou uma infraestrutura de rede que consistia de duas redes LAN (cada uma com 50 computadores), diversos nós de rede interligados representando a internet, além de dois servidores HTTP e FTP.

Para medir a qualidade de serviço, foram coletadas as métricas críticas para os diferentes cenários. No Quadro 4 estão dispostas as métricas coletadas durante o experimento em cada cenário.

Quadro 4 – Métricas críticas em cada cenário

Cenário	Métricas críticas
VoIP e videoconferência	*Delay* e *jitter*
HTTP	Tempo de resposta do objeto HTTP e tempo de resposta de página HTTP
FTP	Tempo de resposta de download FTP e Tempo de resposta de upload FTP

Fonte: Elaborado pelo autor, baseado em (Sllame, 2022).

Além disso, também foi levado em conta o atraso dos protocolos de rede IP, H.323(no cenário de VoIP e videoconferência), TCP e OSPF. Ao analisar as métricas foi possível observar que o IPSec teve melhor desempenho do que o MPLS VPN nos cenários apresentados. Entretanto, foi possível constatar que isso se deu por conta que o MPLS VPN sofreu maiores atrasos por causa do tempo de processamento dos protocolos mencionados.

O trabalho descrito de Sllame (2022), apresenta similaridade com esta pesquisa, tendo em vista que o autor também aborda uma comparação de desempenho entre soluções VPN em aplicações sensíveis a latência, como é o caso das videoconferências.

3.3 *Network Performance Evaluation of VPN Protocols (SSTP and IKEv2)*

O trabalho de Lawas *et al.* (2016), avalia o desempenho dos protocolos VPN SSTP e IKEv2. O experimento foi montado usando quatro computadores, sendo dois clientes e dois servidores. Os testes foram realizados em um ambiente de rede cabeada rodando o protocolo IPv4, onde dois servidores e um cliente estavam ligados na mesma rede, e o outro cliente ligado ao servidor VPN.

Para avaliar a qualidade de serviço, foram coletadas as métricas de *delay*, *jitter* e *throughput*, além do atraso dos protocolos UDP e TCP. Para gerar tráfego de rede, foi usada a

ferramenta D-ITG instalada em ambos os clientes. Além disso, foi usada a própria ferramenta D-ITG para coletar os dados.

Ao fim do experimento, e baseando-se nas métricas coletadas, foi possível constatar que o IKEv2, no geral, performou significativamente melhor que o SSTP nas três métricas mencionadas. Os autores mencionam ainda a possibilidade de estender a pesquisa para outros protocolos VPN e sistemas operacionais.

O trabalho descrito de Lawas *et al.* (2016) pode ser relacionado com esta pesquisa pois descreve um experimento comparativo de desempenho entre duas soluções VPN. Embora o trabalho não seja dedicado a aplicações de baixa latência, como já descrito, os autores coletaram algumas das métricas críticas para essas aplicações.

3.4 *Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol*

O trabalho de Budiyanto e Gunawan (2023) descreve uma análise comparativa de desempenho de protocolos de tunelamento de camada 2 sobre VoIP. As soluções abordadas no estudo foram os protocolos GRE+IPSec, IPIP-BASED, L2TP+IPSec e SSLVPN, em um ambiente de rede cabeada real consistindo de 1 servidor VoIP, 3 roteadores, 3 *switches* e usuários.

Para medir a qualidade de serviço, os autores coletaram métricas de *delay*, *jitter*, *packet loss* e *throughput*. Os dados foram obtidos nas máquinas cliente usando a ferramenta Wireshark, que permite capturar o tráfego da rede de forma detalhada. A coleta teve uma duração total de 5 dias, durante o expediente padrão, que corresponde ao horário comercial praticado pela maioria das empresas, das 8:00h às 16:00h.

Ao fim do experimento, foi possível constatar que as quatro soluções testadas apresentaram resultados estáveis em todos os cenários. De acordo com os autores, a solução que apresentou melhor desempenho foi a SSL VPN. Também foi possível concluir que as soluções que tiveram a adição do IPSec apresentaram um desempenho inferior, pois este causou um elevado consumo de recursos computacionais por conta do processo de criptografia usado para aumentar a segurança.

3.5 Visão geral

Esta seção oferece uma visão geral das técnicas e métricas abordadas pelos autores, como é possível observar no Quadro 5.

Quadro 5 – Visão geral dos trabalhos relacionados

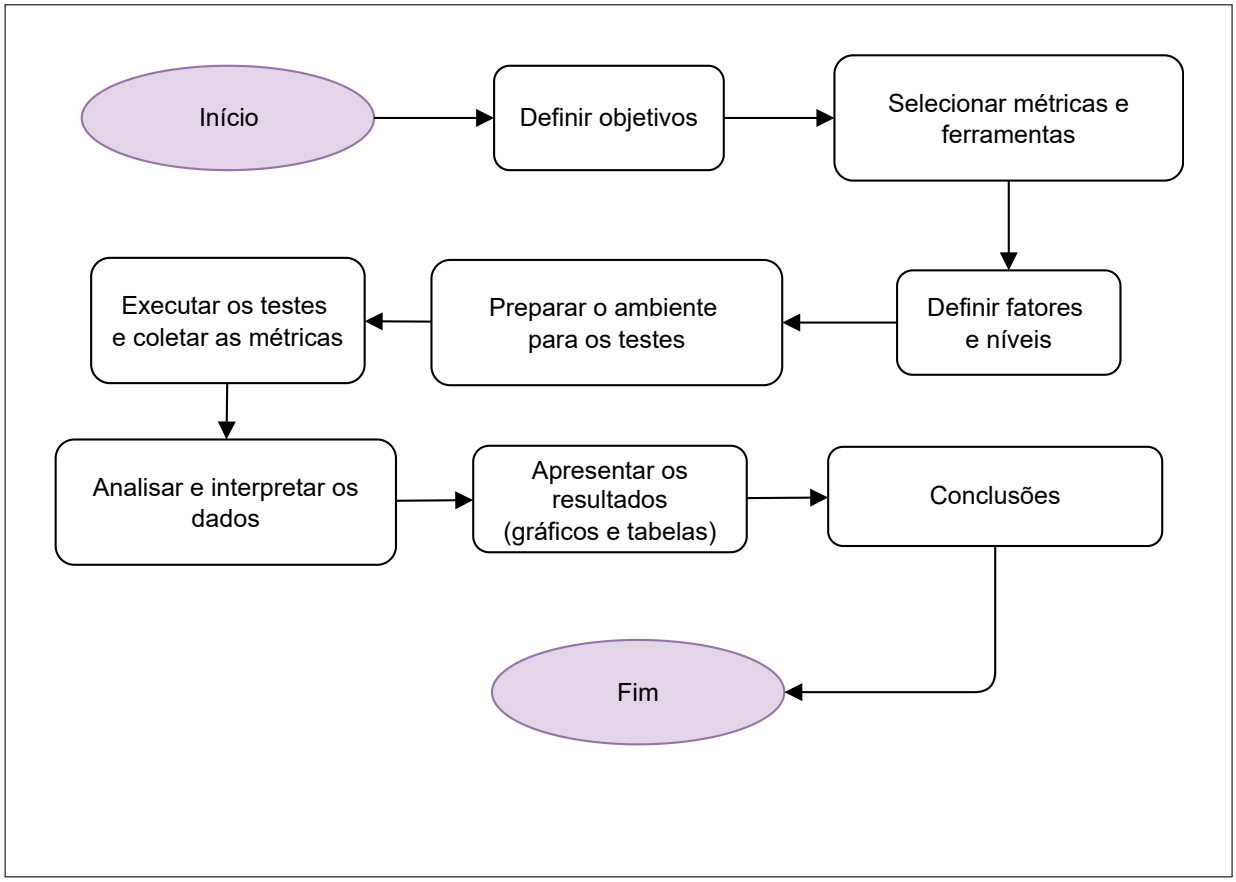
Trabalho	**Tipo de experimento**	**Objetos de estudo**	**Métricas**	**Orientado a aplicações sensíveis à latência?**
Wahanani *et al.* (2021)	Simulação	L2TP/IPSec OpenVPN	*Delay* *Jitter* *Throughput* *Packet loss*	Sim
Sllame (2022)	Simulação	MPLS VPN IPSec	*Delay* *Jitter*	Parcialmente
Lawas *et al.* (2016)	Aferição em ambiente real	SSTP IKEv2	*Delay* *Jitter* *Throughput* *Packet loss*	Não
Budiyanto e Gunawan (2023)	Aferição em ambiente real	GRE+IPSec IPIP-BASED L2TP+IPSec SSLVPN	*Delay* *Jitter* *Throughput* *Packet loss*	Sim
Esta pesquisa	Emulação e virtualização	OpenVPN WireGuard	*Interarrival* *Jitter* *Throughput* *Bitrate* *Packet loss* *Playback continuity*	Sim

Fonte: Elaborado pelo autor.

4 METODOLOGIA

Nesse capítulo será descrita a metodologia usada para conduzir os testes de avaliação das ferramentas OpenVPN e WireGuard, bem como os passos da abordagem sistemática usada durante o trabalho. Serão também apresentadas as variáveis presentes no experimento além da configuração do mesmo, destacando as ferramentas de medição e a topologia usada. A Figura 5 mostra os passos para a abordagem sistemática deste trabalho.

Figura 5 – Passos para a abordagem desse trabalho



Fonte: Elaborado pelo autor.

4.1 Definir objetivos

A etapa da definição de objetivos é uma parte fundamental de todo experimento. Além da definição de metas, nessa etapa também são apresentadas as motivações e delimitações do experimento. Os objetivos que regem este trabalho já foram previamente apresentados e discutidos no Capítulo 1.

4.2 Selecionar métricas e ferramentas

Nessa seção serão listadas as métricas coletadas durante o experimento. As métricas de *interarrival*, *jitter* e *packet loss* foram coletadas durante a transmissão do vídeo, por meio da captura do tráfego VPN usando a ferramenta Tshark na máquina do cliente. A métrica de *playback continuity* foi obtida através da análise dos *logs* da ferramenta de *streaming* e reprodução de vídeo, o VLC.

4.2.1 Escolha das métricas

- *Interarrival*: O atraso entre a chegada de dois pacotes consecutivos. Impacta a experiência do usuário, um atraso muito alto pode ocasionar travamentos na voz e vídeo transmitidos. O cálculo do *interarrival* pode ser expresso por

$$I_i = t_i - t_{i-1}. \tag{4.1}$$

- *Jitter*: É a variação do atraso, o que pode se traduzir como a constância em que a conexão permanece estável ou não. O *jitter* pode ser calculado por

$$J_i = |I_i - I_{i-1}|. \tag{4.2}$$

- *Packet loss*: Um *delay* muito alto pode ocasionar com que os pacotes sejam descartados em algum ponto da rede. Isso se traduz como falha na conexão ou travamentos. O cálculo de pacotes perdidos se dá por

$$PL = \frac{P_{\text{perdidos}}}{P_{\text{enviados}}} \times 100. \tag{4.3}$$

- *Throughput*: A vazão de pacotes, o quanto efetivamente a rede consegue transportar sem que ocorram perdas ou atrasos. Influencia em quantas chamadas simultâneas o servidor VPN consegue suportar. O throughput pode ser calculado por

$$T = \frac{B_{\text{recebidos}}}{\Delta t}. \tag{4.4}$$

  Quando expresso em megabits por segundo (Mbps), o throughput é dado por

$$T_{\text{Mbps}} = \frac{B_{\text{recebidos}}}{\Delta t \times 10^6}. \tag{4.5}$$

- *Bitrate*: O *bitrate* corresponde ao total de bits gerados pela aplicação durante a reprodução do vídeo.
- *Playback continuity*: Corresponde ao quão fluidos a voz e vídeo estão durante a transmissão.

4.2.2 Escolha das ferramentas

- Oracle VirtualBox: Foi usado para virtualizar as máquinas do experimento na máquina hospedeira.
- Tshark: Foi usado na máquina cliente VPN para coletar as métricas do experimento.
- Google Colab: Um jupyter notebook que foi usado para criar os gráficos.
- Python3: Foi usado para filtrar as métricas do arquivo de captura do Tshark, e *logs* do VLC, bem como realizar seus respectivos cálculos.
- VLC: Foi usado como gerador de tráfego RTP no servidor, bem como receptor do tráfego no cliente.

4.3 Definir fatores e níveis

Essa etapa consiste na análise e identificação das variáveis que podem influenciar nos resultados do experimento, bem como os níveis, que são as variações entre os cenários de testes. A seguir serão listadas as variáveis e suas influências no experimento.

- Rede: Em ambientes reais a própria rede é uma variável, pois os resultados do experimento seriam diretamente influenciados pela estabilidade da mesma, além da distância física entre os dois *hosts*. Este experimento visa comparar diretamente as duas soluções VPN, portanto essa variável precisa ser removida. Para contornar este problema, a solução adotada foi executar o experimento em máquinas virtuais sendo executadas em uma mesma máquina hospedeira. Em ambientes reais, seria desejável que os *hosts* estivessem fisicamente o mais próximos possível, a poucos metros de distância.
- Máquinas virtuais: Devido a limitações inerentes ao seu funcionamento, as máquinas virtuais podem apresentar travamentos ou instabilidade, o que pode influenciar as métricas do experimento. Monitoramento constante e a coleta de um volume elevado de dados foram as soluções adotadas para contornar este problema.
- Máquina hospedeira: Os recursos da máquina hospedeira afetam diretamente a estabilidade das máquinas virtuais, o que pode acarretar em travamentos durante o experimento. A máquina hospedeira usada neste experimento será descrita na subseção 4.4.1.

Para este experimento, os níveis correspondem às qualidades de vídeo 360p, 480p, 720p e 1080p e às duas soluções VPN em estudo. O Quadro 6 mostra a disposição dos níveis do experimento.

Quadro 6 – Testes a serem realizados

Tecnologia	Teste
OpenVPN	Vídeo 360p Vídeo 480p Vídeo 720p Vídeo 1080p
WireGuard	Vídeo 360p Vídeo 480p Vídeo 720p Vídeo 1080p

Fonte: Elaborado pelo autor.

4.4 Preparar o ambiente para os testes

A seguir, serão detalhados os recursos da máquina física que foi responsável por hospedar as máquinas virtuais. É importante evidenciar que os resultados podem variar dependendo dos recursos de cada máquina hospedeira, pois a mesma influencia o desempenho das máquinas virtuais. Isso é um fator importante para a repetibilidade dos testes.

4.4.1 Recursos da máquina hospedeira

Para a realização deste experimento, foi utilizado como máquina hospedeira um *laptop* Acer Nitro 5, modelo AN517-52[1], equipado com processador Intel® Core™ i5-10300H (quad-core, 2,50 GHz), dois módulos de memória RAM DDR4 de 8 GB, totalizando 16 GB, com frequência de 2933 MHz e uma GPU dedicada Nvidia GeForce® GTX 1650 com 4 GB de memória dedicada GDDR5 . O sistema operacional utilizado na máquina hospedeira foi o Windows 11 (64 bits).

4.4.2 Recursos das máquinas virtuais

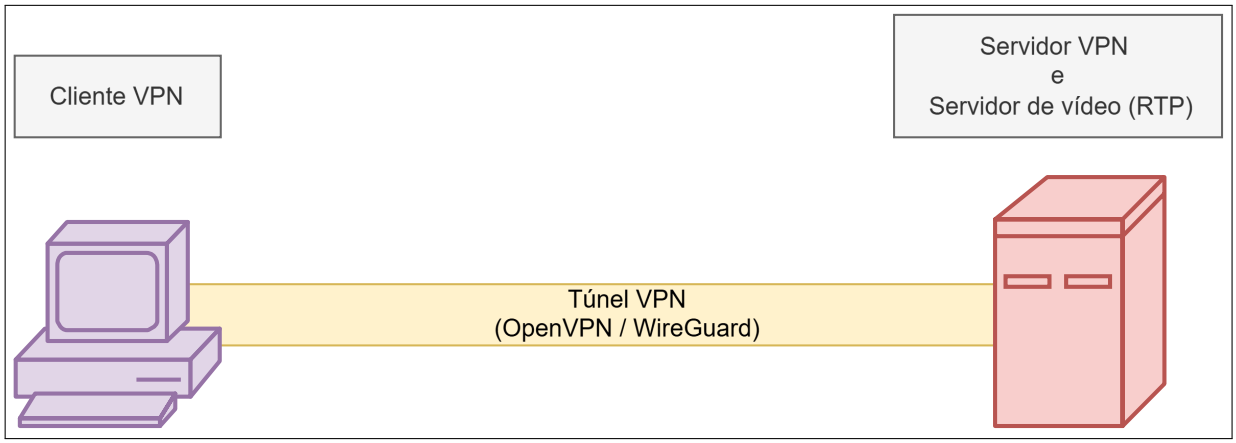
As máquinas virtuais usarão apenas os recursos mínimos para o seu correto funcionamento. Para tal, foram realizados testes preliminares do cenário que mais demandava recursos computacionais, para determinar o melhor valor de memória RAM alocada e núcleos de processamento para cada máquina. Concluiu-se que 2 GB de memória RAM alocada para cada máquina, 2 núcleos de processamento para os servidores e 1 núcleo de processamento para os clientes, garantiriam uma estabilidade constante na execução do experimento definitivo. Os sistemas operacionais usados são baseados no Ubuntu 22.04 LTS *Desktop*.

[1] acer.com

4.4.3 Topologia de rede

A topologia de rede do ambiente de testes consiste em um cliente VPN e de um servidor VPN e *streaming* de vídeo RTP. O cliente VPN acessa a transmissão do servidor de vídeo por meio do túnel VPN, por fim os pacotes de rede serão capturados pelo cliente para análise posterior. A topologia pode ser melhor visualizada na Figura 6.

Figura 6 – Topologia de rede do experimento



Fonte: Elaborado pelo autor.

4.5 Executar os testes e coletar métricas

Após a devida instalação e configuração de todas as ferramentas que seriam usadas durante o experimento, foi então então criado um *snapshot* do ambiente virtual de cada máquina. Um *snapshot* consiste em salvar o estado atual da máquina, sendo assim possível voltar para aquele estado sempre que desejado, isso evita possíveis interferências entre os demais cenários.

Os testes consistiram em iniciar os serviços VPN e o VLC nas máquinas cliente e servidor. Após isso, inicia-se a transmissão RTP do vídeo no servidor para o cliente pelo túnel VPN. O cliente então, recebe o vídeo e usa a ferramenta Tshark para capturar o tráfego da VPN. Também foram usados os *logs* do VLC para a coleta de métricas.

Cada cenário foi executado 8 vezes, com uma duração de 1 hora contínua por execução e 8 horas no total. O objetivo dessa separação é de evitar possíveis problemas com travamentos durante a execução ou possíveis erros do tipo *OOM Killer*, que possam ocorrer devido ao tamanho elevado em disco do arquivo de captura do Tshark. Após finalizada a execução de 1 hora, os resultados serão salvos e extraídos da máquina virtual, em seguida o ambiente é revertido para o estado da *snapshot* e então executado novamente, até concluir as 8

horas totais do cenário. Toda a parte de cálculo e automação do tempo de execução e captura são controlados usando *scripts* Python3 e Shell. No Quadro 7 estão dispostas as métricas coletadas e suas respectivas fontes.

Quadro 7 – Métricas coletadas e respectivas fontes

Categoria	**Métricas**	**Fonte dos dados**
QoE	*Playback continuity*	Logs do VLC
QoS	*Interarrival* *Jitter* *Packet loss* *Throughput*	Arquivos de captura (TShark)
QoS (Complementar)	*Bitrate*	Logs do VLC

Fonte: Elaborado pelo autor.

4.6 Analisar e interpretar os dados coletados

O processo de análise consistiu em extrair as métricas dos arquivos de captura e *logs* usando a linguagem de programação Python3. Após isso, ainda usando a mesma linguagem, foram calculadas as médias e porcentagens usando suas respectivas fórmulas matemáticas. Por fim, os resultados serão apresentados em maior detalhe nos capítulos seguintes, que correspondem ao Capítulo 5 e Capítulo 6.

A ferramenta Tshark não possui interface gráfica, o que significa que não é possível gerar gráficos diretamente por ela. Portanto, a ferramenta Google Colab foi usada para gerar os gráficos e calcular os indicadores estatísticos. O Google Colab usa a tecnologia Jupyter Notebook, um ambiente interativo que usa principalmente a linguagem de programação Python3 para a análise de dados.

4.7 Apresentar os resultados (gráficos e tabelas)

Nessa etapa são expostos os resultados observados ao fim do experimento, de forma clara e objetiva. Para tal, serão usados gráficos para auxiliar na visualização dos resultados. O Capítulo 5 corresponde a este passo da abordagem sistemática.

5 RESULTADOS

Nesse capítulo serão expostos e consolidados os resultados dos distintos cenários do experimento, bem como suas respectivas análises. Para que seja possível realizar uma análise de desempenho com base nas métricas, é necessário estabelecer limiares para as mesmas. Para esse trabalho serão usados os limiares de QoS estabelecidos na *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) (ETSI, 2002).

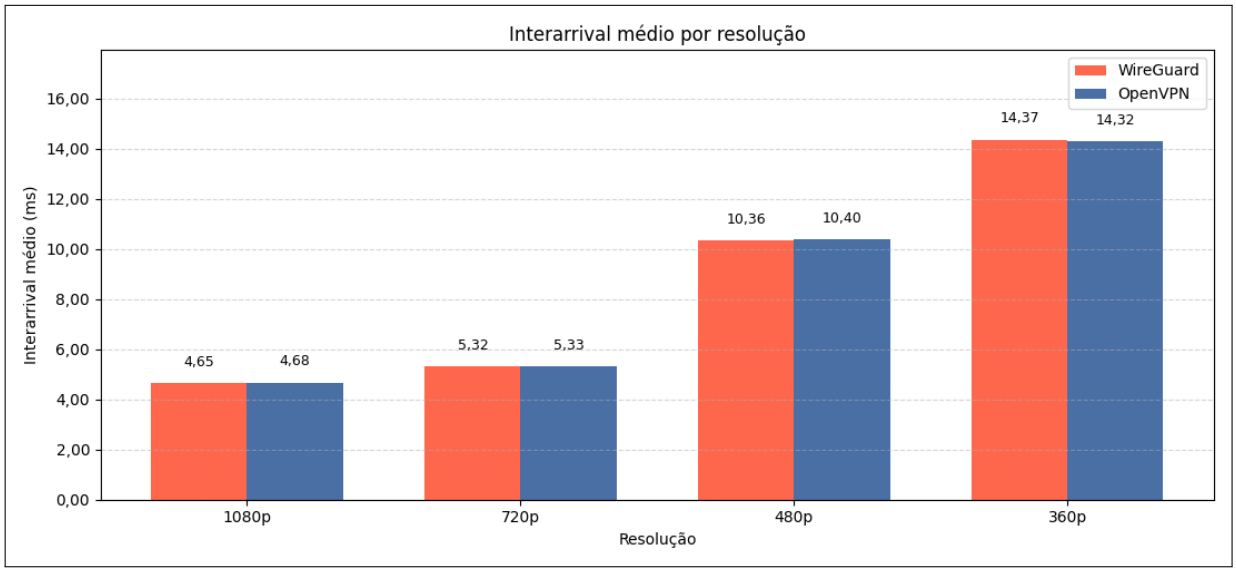
5.1 Métricas de QoS

Essa seção é dedicada a análise das métricas de Qualidade de Serviço. Em cada subseção serão apresentados os limiares segundo ETSI (2002), bem como a análise dos resultados.

5.1.1 Interarrival

Ao final das 8 horas totais de execução de cada cenário foi possível constatar que o *interarrival* de ambas as soluções VPN em estudo, apresentaram valores similares entre os cenários equivalentes. Os gráficos da Figura 7 evidenciam esse fato.

Figura 7 – Resultados de *Interarrival* por cenário



Fonte: Elaborado pelo autor.
Nota: Os valores apresentados representam as médias após consolidadas as 8 horas de cada cenário.

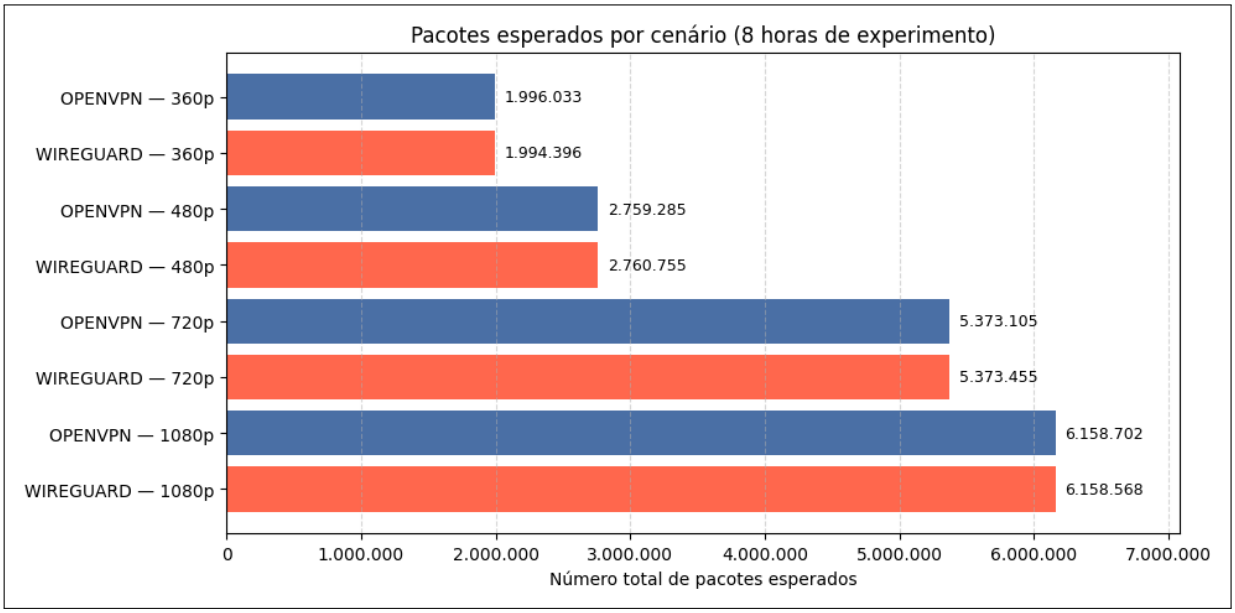
Diante do que foi observado, embora não seja possível estabelecer uma comparação direta entre a métrica de *interarrival* e o atraso fim-a-fim, o que inviabiliza a aplicação dos limiares definidos por ETSI (2002), optou-se por apresentar esses valores como referência

qualitativa. Nesse contexto, os resultados obtidos indicam valores satisfatórios, pois as médias apresentam valores muito próximos entre os cenários equivalentes.

Esse comportamento indica que o tráfego está sendo empacotado de forma semelhante nas duas soluções VPN, uma vez que os valores de *interarrival* apresentaram padrões próximos entre os cenários equivalentes. Isso sugere que os mecanismos de encapsulamento adotados não introduzem alterações significativas entre si na cadência de envio dos pacotes, preservando o comportamento temporal imposto pelo VLC.

Observa-se que o aumento do *interarrival* à medida que a resolução do vídeo diminui ocorre em função da própria característica do tráfego gerado. Resoluções mais baixas demandam menor volume de dados, resultando em menor quantidade de pacotes transmitidos, o que implica maiores intervalos de tempo entre pacotes consecutivos, como atestado na Figura 8. Assim, esse comportamento não está necessariamente associado a degradações na fluidez da transmissão, mas reflete a adaptação do fluxo de dados à qualidade de vídeo utilizada.

Figura 8 – Total de Pacotes por cenário



Fonte: Elaborado pelo autor.
Nota: O total de pacotes RTP corresponde ao número de pacotes esperados, obtido a partir do intervalo do número de sequência presente no cabeçalho RTP.

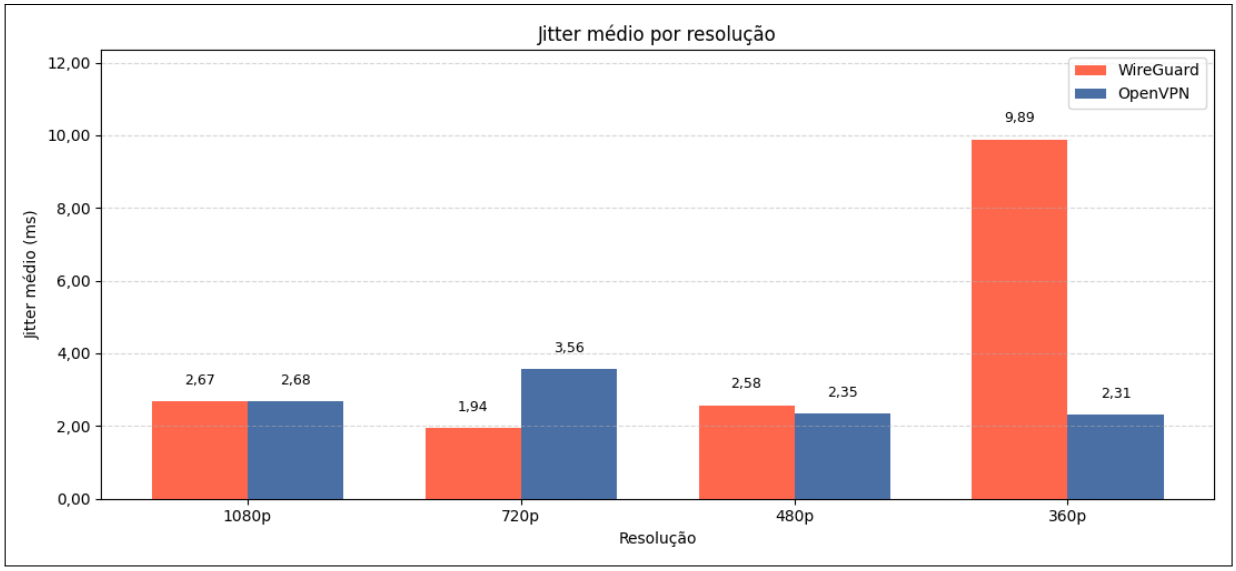
5.1.2 Jitter

No cenário de testes do OpenVPN o *jitter* médio apresentou valores baixos e estáveis em todas as resoluções de vídeo testadas. O comportamento observado evidencia que mesmo com o aumento de carga na rede causada pelas resoluções de vídeo mais altas, o OpenVPN foi

capaz de entregar os pacotes com baixa variação temporal.

No cenário de testes do WireGuard, a solução VPN em questão apresentou estabilidade nas resoluções de vídeo 480p, 720p, e 1080p, e em alguns casos apresentou valores mais baixos comparados ao OpenVPN. Entretanto, é possível notar que houve um aumento significativo na média dos valores no cenário da resolução 360p. Esse comportamento atípico pode sugerir que algum fator externo como instabilidade do túnel VPN, ou mesmo características específicas do encapsulamento do WireGuard e agendamento de pacotes que podem ter afetado a estabilidade nesse cenário específico. No gráfico da Figura 9 estão dispostos os resultados do *jitter* por resolução de vídeo. Cada barra do gráfico corresponde ao intervalo de 8 horas de execução dos seus respectivos cenários.

Figura 9 – Resultados de *Jitter* médio por cenário



Fonte: Elaborado pelo autor.
Nota: Os valores apresentados representam as médias após consolidadas as 8 horas de cada cenário.

Diante do que foi demonstrado, é possível concluir que embora o WireGuard tenha apresentado uma variação pontual no cenário referente a resolução de vídeo 360p, a solução VPN em questão se mostrou ligeiramente mais eficiente nas resoluções mais altas, 720p e 1080p. Tomando como base os limiares estabelecidos em ETSI (2002), ambas as soluções VPN mostraram valores de *jitter* satisfatórios, como é possível observar no Quadro 8.

Quadro 8 – Classificação de *Jitter*

***Jitter* (ms)**	**Categoria**
0 ms	Muito bom
0 ms a 75 ms	Bom
75 ms a 125 ms	Regular
125 ms a 225 ms	Ruim

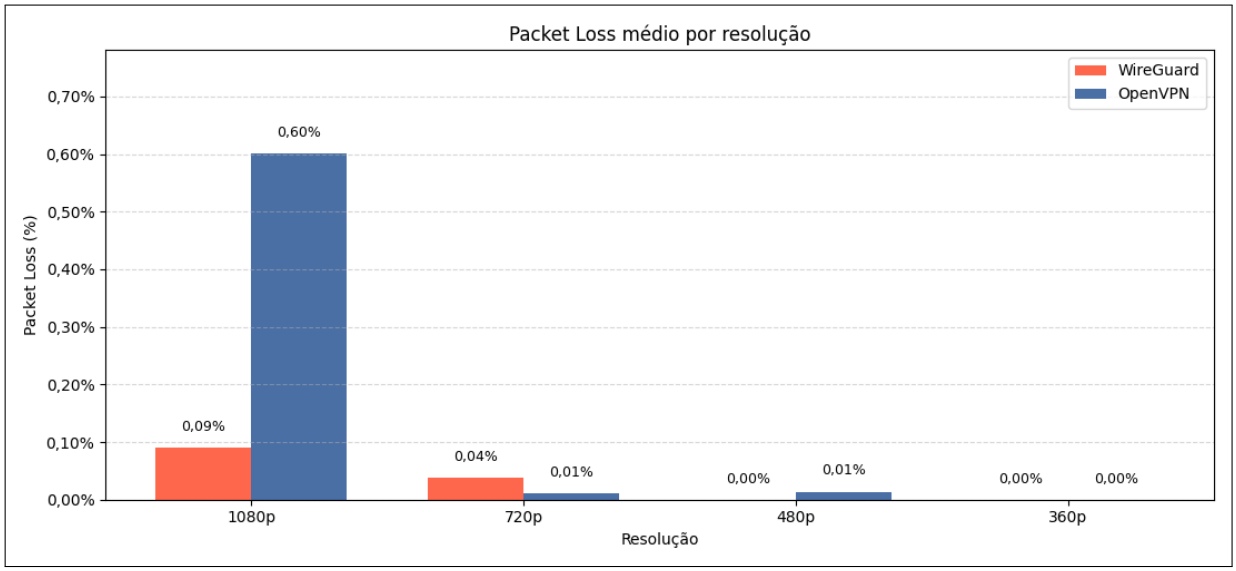
Fonte: Adaptado de (ETSI, 2002).

5.1.3 Packet loss

No cenário de testes do WireGuard, a solução VPN mostrou-se robusta durante os testes de todas as qualidades de vídeo, apresentando perdas mínimas mesmo na maior qualidade de vídeo testada, 1080p. Esse comportamento evidencia a estabilidade apresentada pelo WireGuard durante o experimento.

O OpenVPN, entretanto, embora tenha apresentado perdas mínimas na maioria das resoluções de vídeo testadas, mostrou-se mais suscetível a perda de pacotes em cargas maiores. No cenário de maior carga, foi possível observar um aumento expressivo na perda de pacotes em comparação com as outras resoluções de vídeo. O gráfico da Figura 10 evidencia esse comportamento.

Figura 10 – Porcentagem de perdas de pacote *(packet loss)*



Fonte: Elaborado pelo autor.
Nota: Os as porcentagens apresentadas correspondem às 8 horas de duração total de cada cenário.

Ao comparar as duas soluções VPN, é evidente que o WireGuard apresentou uma menor perda de pacotes do que o OpenVPN no geral. Tal comportamento pode ser atribuído ao maior *overhead* do OpenVPN, além do encapsulamento adicional causado pela demanda

do tráfego de vídeo em 1080p. Entretanto, segundo os limiares definidos em ETSI (2002), os valores apresentados por ambas as soluções VPN em estudo são considerados satisfatórios, como é possível observar no Quadro 9.

Quadro 9 – Classificação de Packet Loss

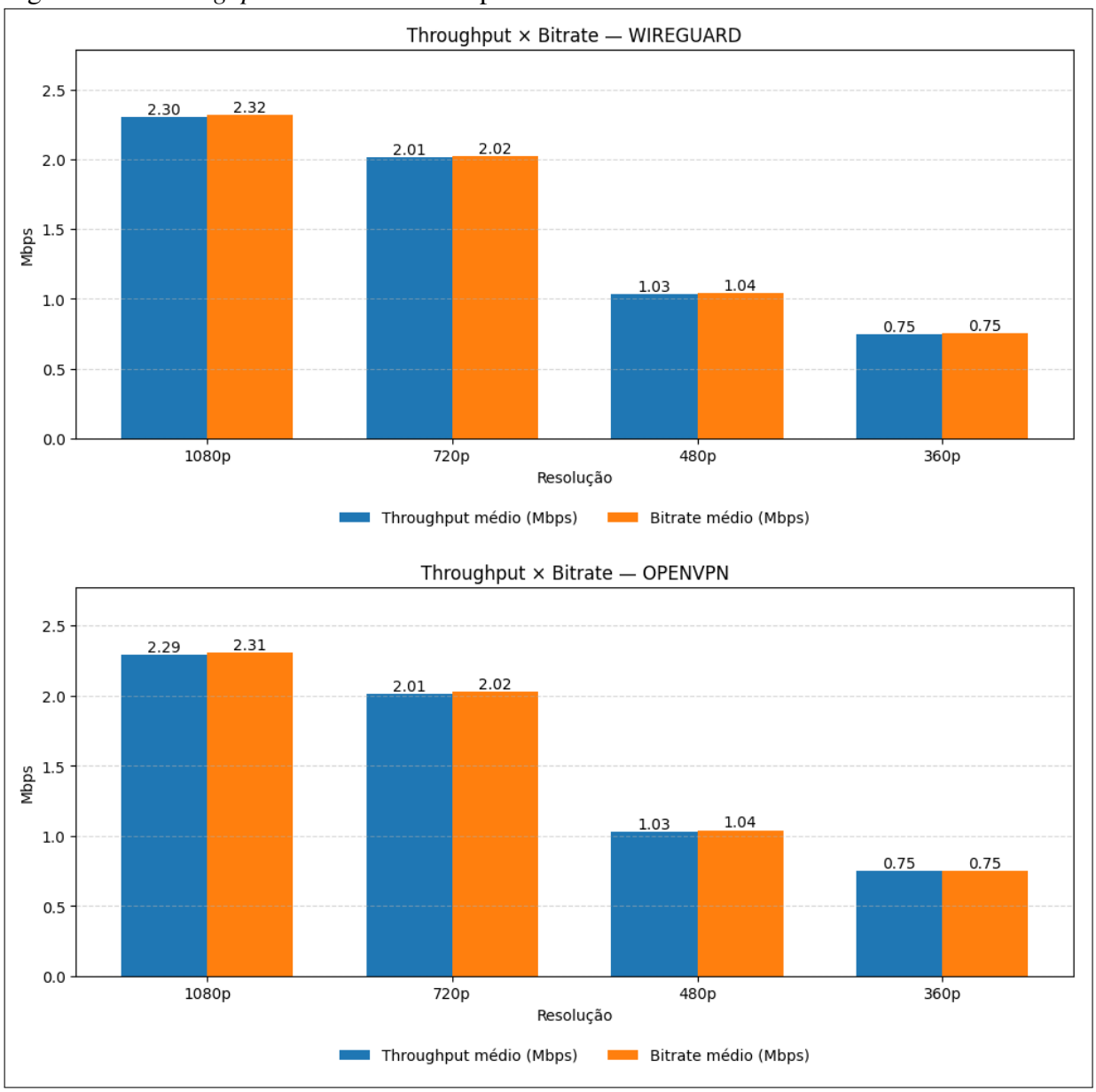
Packet Loss (%)	**Categoria**
0 %	Muito bom
0% a 3 %	Bom
3% a 15 %	Regular
> 25 %	Ruim

Fonte: Adaptado de (ETSI, 2002).

5.1.4 Throughput e Bitrate

Ao analisar os resultados do teste de *throughput*, é possível constatar que ambas as soluções VPN apresentaram valores praticamente idênticos entre as resoluções de vídeo testadas. É possível constatar que os valores de ambas as métricas estão extremamente próximos. Esse comportamento evidencia que ambas as soluções VPN foram perfeitamente capazes de sustentar o fluxo de vídeo, de forma a atender a demanda em cada cenário, como é mostrado nos gráficos da Figura 11.

Figura 11 – *Throughput* e *Bitrate* médios por cenário de testes



Fonte: Elaborado pelo autor.

No contexto desse trabalho, a métrica de *throughput* está sendo limitada apenas pelo *bitrate* do vídeo transmitido. Dessa forma, o valor de 100% representa o *bitrate* nominal do fluxo de vídeo. Segundo os limiares definidos em ETSI (2002) o quão mais próximo o valor apresentado pelo *throughput* estiver desse valor de referência, melhor será a qualidade de serviço. No Quadro 10 estão dispostos os limiares em questão.

Quadro 10 – Classificação de *Throughput*

***Throughput* (%)**	**Categoria**
75% a 100%	Muito bom
50% a 75%	Bom
25% a 50%	Regular
$< 25\%$	Ruim

Fonte: Adaptado de (ETSI, 2002)

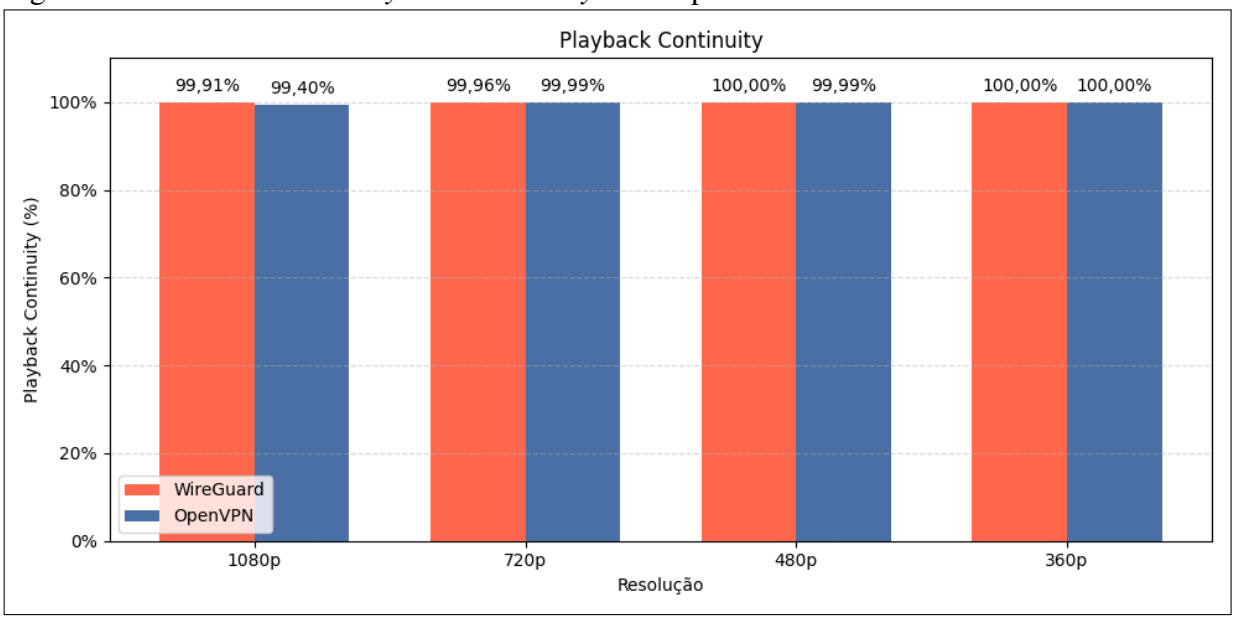
5.2 Métricas de QoE

Diferentemente das métricas de Qualidade de Serviço, não é possível encontrar na literatura valores universais para as métricas de Qualidade de Experiência. Isso se dá porque cada usuário percebe o desempenho da reprodução de vídeo de maneira diferente. Essa singularidade torna impossível estabelecer limiares universais para as métricas de QoE, sendo assim, os valores apresentados nesta seção não devem ser tratados como absolutos, eles apenas representam um comparativo entre os dois distintos cenários deste experimento.

5.2.1 Playback continuity

Ainda que não seja possível estabelecer limiares universais para a métrica de *playback continuity*, fica evidente por meio do gráfico da Figura 12 que ambas soluções VPN em estudo apresentaram uma elevada continuidade de reprodução em todas as resoluções de vídeo testadas. O comportamento observado sugere que o funcionamento das VPNs não impactou de forma significativa o usuário, pois quanto mais próximo de 100% está um valor, maior será a fluidez observada durante a transmissão.

Figura 12 – Resultados de *Playback continuity* médio por cenário



Fonte: Elaborado pelo autor.

6 CONCLUSÕES E TRABALHOS FUTUROS

A ampla adoção dos serviços de videochamadas causada pelo rápido crescimento das modalidades de *home office* e EAD trouxeram consigo preocupações quanto à segurança e confidencialidade da informação transmitida na rede durante o uso do serviço. As VPNs, que surgiram como uma alternativa de baixo custo para interligar duas redes privadas distantes, rapidamente evoluíram para também prover confidencialidade do tráfego usando o túnel lógico criptografado.

A fim de quantificar os impactos causados pelas VPNs em serviços de videochamadas, este trabalho analisou o desempenho de duas soluções VPN modernas, o OpenVPN e o WireGuard. Ao final dos experimentos, foi possível constatar que ambas as soluções VPN mostraram-se capazes de entregar uma elevada qualidade de serviço diante dos distintos cenários de carga representados pelas qualidades de vídeo. Além disso, ambas as soluções VPN estudadas destacam-se por sua constante atualização e suporte, bem como a facilidade de instalação e configuração das mesmas.

Como trabalhos futuros, sugere-se a realização do experimento usando ferramentas de videochamadas dedicadas, como é o caso da ferramenta Jitsi. Propõe-se também testes com maior número de clientes e a realização de pesquisas com os usuários finais para auxiliar na definição de limiares para métricas de QoE para esse experimento. E ainda, se possível, a realização de testes em um ambiente físico, com equipamentos e usuários reais.

REFERÊNCIAS

ACETO, G.; PERSICO, V.; PESCAPÉ, A. Internet censorship detection: A survey. **Computer Networks**, Elsevier, v. 83, p. 432–454, 2015.

BUDIYANTO, S.; GUNAWAN, D. Comparative analysis of vpn protocols at layer 2 focusing on voice over internet protocol. **IEEE Access**, v. 11, p. 60853–60865, 2023.

CHACON, S.; BENHADDOU, D.; GURKAN, D. Secure voice over internet protocol (voip) using virtual private networks (vpn) and internet protocol security (ipsec). In: 2006 IEEE REGION 5 CONFERENCE. **Proceedings [...]**. Texas, USA: Institute of Electrical and Electronics Engineers, 2006. p. 218–222.

ETSI. **Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); End-to-end Quality of Service in TIPHON Systems; Part 7**: Design guide for elements of a tiphon connection from an end-user perspective. Sophia Antipolis, 2002.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet**: uma abordagem top-down. 8. ed. São Paulo: Pearson, 2021. ISBN 9788582605592.

LAWAS, J. B. R.; VIVERO, A. C.; SHARMA, A. Network performance evaluation of vpn protocols (sstp and ikev2). In: WORLD MULTICONFERENCE ON SYSTEMICS, CYBERNETICS AND INFORMATICS. **Proceedings [...]**. Hyderabad, India: Institute of Electrical and Electronics Engineers, 2016. p. 1–5.

OpenVPN Technologies, Inc. **OpenVPN Community Documentation**. 2025. Disponível em: https://openvpn.net/community-docs/. Acesso em: 28 jun. 2025.

RANI, U.; DHIR, R. K.; FURRER, M.; GőBEL, N.; MORAITI, A.; COONEY, S.; MANUS, A. C. M. **Working Time and Digitalization**: The future of work in a changing economy. Geneva: International Labour Office, 2021. ISBN 978-92-2-031941-3.

SCHAEVITZ, S. **Three months, 30x demand**: How we scaled google meet during covid-19. Google Workspace Blog, 2020. Disponível em: https://workspace.google.com/blog/productivity-collaboration/keeping-google-meet-ahead-of-usage-demand-during-covid-19. Acesso em: 1 jun. 2025.

SLLAME, A. M. Performance evaluation of multimedia over mpls vpn and ipsec networks. In: 2022 IEEE 2ND INTERNATIONAL MAGHREB MEETING OF THE CONFERENCE ON SCIENCES AND TECHNIQUES OF AUTOMATIC CONTROL AND COMPUTER ENGINEERING (MI-STA). **Proceedings [...]**. Sabratha, Libya: Institute of Electrical and Electronics Engineers, 2022. p. 32–37.

STALLINGS, W. **Network Security Essentials**: Applications and standards. 6. ed. Boston: Pearson, 2021. ISBN 9780137561650.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. J. **Computer Networks, Global Edition**. 6. ed. [*S. l.*]: Pearson Higher Ed, 2021. EBook. ISBN 9781292374017.

WAHANANI, H. E.; IDHOM, M.; MANDYARTHA, E. P. Analysis of streaming video on vpn networks between openvpn and l2tp/ipsec. In: 2021 IEEE 7TH INFORMATION TECHNOLOGY INTERNATIONAL SEMINAR (ITIS). **Proceedings[...]**. Surabaya, Indonesia: Institute of Electrical and Electronics Engineers, 2021. p. 1–5.

WireGuard Development Team. **WireGuard Documentation**. 2025. Disponível em: https://www.wireguard.com/. Acesso em: 28 jun. 2025.