

Medição do impacto de uma infraestrutura de VPN na taxa de transmissão e na latência

ESTER CRESTANI, GABRIEL PEREIRA E JÚLIA PIMENTEL, ESTER CRESTANI, GABRIEL PEREIRA, and JULIA PIMENTEL

Este estudo teve como objetivo avaliar o impacto da infraestrutura de VPN da UFRGS, baseada em OpenVPN, no desempenho de rede. Foram realizadas medições de vazão (throughput), latência, jitter e perda de pacotes em computadores pessoais dos integrantes do grupo, utilizando iperf, ping e scripts em Python para automatizar as coletas nos cenários com e sem VPN, em diferentes horários do dia. Os resultados mostraram que o uso da VPN, em geral, reduz a vazão tanto de download quanto de upload e tende a aumentar a latência e a variabilidade do atraso, enquanto a perda de pacotes apresenta indícios de piora com a VPN ligada, ainda que dependente de coletas mais robustas. Conclui-se, portanto, que a infraestrutura de VPN analisada introduz overhead perceptível nas principais métricas de desempenho, confirmando o impacto do uso de VPN na qualidade da conexão sob condições reais de utilização.

ACM Reference Format:

Ester Crestani, Gabriel Pereira e Júlia Pimentel, Ester Crestani, Gabriel Pereira, and Julia Pimentel. 2025. Medição do impacto de uma infraestrutura de VPN na taxa de transmissão e na latência. 1, 1 (December 2025), 10 pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

1 INTRODUÇÃO

Este trabalho foi desenvolvido na disciplina de Avaliação de Desempenho do curso de Engenharia de Computação da UFRGS, tendo como objetivo aplicar, em um sistema real, os conceitos de medições de desempenho estudados em aula. O objeto de estudo é a infraestrutura de VPN (Virtual Private Network) disponibilizada pela universidade, acessada por meio do protocolo OpenVPN e utilizada pela comunidade acadêmica para acesso remoto seguro a serviços institucionais e recursos restritos à rede interna

As redes privadas virtuais vêm se tornando cada vez mais importantes em ambientes acadêmicos e corporativos, pois adicionam uma camada de criptografia e encapsulamento ao tráfego de dados. No entanto, essa camada extra pode introduzir overhead na comunicação e afetar a qualidade da conexão. Nesse contexto, este trabalho investiga, de forma prática, como o uso de VPN impacta o desempenho de rede, com foco em quatro métricas: vazão (throughput), latência, jitter e perda de pacotes.

Para isso, são realizadas medições diretas dessas métricas em cenários com e sem uso da VPN da UFRGS, em diferentes horários de utilização. Parte-se da hipótese de que a VPN reduz a vazão disponível e aumenta a latência, o jitter e a perda de pacotes, degradando o

Authors' address: Ester Crestani, Gabriel Pereira e Júlia Pimentel; Ester Crestani; Gabriel Pereira; Julia Pimentel.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM XXXX-XXXX/2025/12-ART

<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

desempenho percebido pelo usuário. O objetivo é quantificar esse impacto e fornecer uma visão clara sobre os efeitos do uso da VPN em condições reais de operação.

2 METODOLOGIA

Nesta seção é apresentada a metodologia utilizada para avaliar o impacto da VPN da UFRGS no desempenho de rede. São descritos o método de análise escolhido, o ambiente de medição, as ferramentas empregadas e o procedimento adotado para a coleta das medições de vazão, latência, jitter e perda de pacotes, em cenários com e sem uso da VPN.

2.1 Ambiente de medição

Os experimentos foram realizados nos computadores pessoais dos integrantes do grupo, conectados à internet residencial, utilizando o cliente OpenVPN e a infraestrutura de VPN disponibilizada pela UFRGS para alunos. Como objeto de estudo, adotou-se essa VPN institucional devido à sua relevância prática no contexto acadêmico e ao fácil acesso pelos participantes.

As medições foram conduzidas em dias e horários distintos, em condições reais de uso, com a VPN conectada e desconectada. Os testes envolveram o acesso a um serviços utilizado rotineiramente pela comunidade acadêmica (moodle), de modo a representar de forma realista o uso típico da VPN e padronizar os experimentos para melhor análise.

2.2 Ferramentas

Para avaliar o desempenho da rede no contexto deste estudo, foram utilizadas principalmente as ferramentas iperf e ping. O iperf foi empregado para medir a vazão (throughput), utilizando o servidor disponibilizado pelo PCAD da universidade como ponto remoto de teste. Os experimentos foram executados em cenários com e sem VPN, permitindo comparar diretamente o impacto do túnel VPN nessas métricas.

Já o ping foi utilizado para medir a latência (RTT), o jitter (de acordo com o RFC 3550) e a perda de pacotes. Para isso, foram realizados testes sempre tendo como destino a plataforma Moodle da UFRGS, de forma a padronizar os experimentos e permitir uma comparação mais consistente entre os cenários com e sem uso da VPN.

2.3 Experimentos

Os experimentos foram realizados a partir de um script em Python desenvolvido especificamente para este trabalho, responsável por executar os testes de desempenho e registrar automaticamente os resultados. O script realiza testes de vazão (throughput) com o iperf e testes de latência e perda de pacotes por meio do ping, salvando os dados em arquivos no formato CSV para posterior análise.

Para garantir que o experimento fosse igualitário entre os participantes e pudesse ser reproduzido, o projeto foi organizado em um repositório no GitHub, contendo o código-fonte e um arquivo de requisitos para instalação das dependências. Cada integrante do grupo executou o script em seu próprio computador, utilizando a mesma versão do código e o mesmo conjunto de parâmetros. Os arquivos de dados gerados foram armazenados em pastas separadas por participante, permitindo a análise individual de cada ambiente de teste.

O script também automatiza o controle do estado da VPN da UFRGS. Durante a execução, ele realiza a conexão e a desconexão da VPN de forma programada, alternando entre períodos com a VPN ativa e inativa. Em cada estado, são executadas sequências de testes de iperf e ping, mantendo a mesma duração e o mesmo padrão de repetição, de modo a tornar comparáveis os resultados obtidos com e sem o uso da VPN. Além disso, parâmetros como

número de ciclos, duração de cada ciclo e tempo total de execução podem ser ajustados no próprio script, o que permite adaptar o experimento ao tempo disponível de coleta sem comprometer a padronização entre os participantes.

3 RESULTADOS

Os resultados dos experimentos foram armazenados em arquivos .csv separados para cada integrante do grupo. A partir desses dados, foi desenvolvido um script em Python para gerar gráficos que sintetizam os resultados de cada amostra, por participante. Esses gráficos permitem visualizar de forma comparativa a influência do uso da VPN sobre as métricas de desempenho analisadas: latência, jitter, vazão e perda de pacotes.

Nas seções a seguir, os resultados são apresentados em subtópicos organizados por métrica, acompanhados dos respectivos gráficos, de modo a facilitar a interpretação do impacto da VPN em cada caso.

Sobre os resultados obtidos, vale salientar que, para as análises de perda de pacotes (loss), optou-se por manter as informações apresentadas na Etapa 2 do trabalho. Essa escolha se deve ao fato de que, nos experimentos mais recentes, o indicador sofreu influência indireta de outras alterações no script e na forma de armazenamento dos dados, o que poderia comprometer a confiabilidade das conclusões. Além disso, no caso das medições realizadas por Ester, o ambiente de coleta foi modificado em função de problemas na máquina pessoal, exigindo o uso de outro equipamento e, consequentemente, introduzindo diferenças adicionais de contexto. Por fim, destaca-se que os resultados apresentam periodicidades distintas entre os membros do grupo. Isso ocorreu porque se buscou controlar o ambiente de rede para cada participante, realizando os testes em momentos compatíveis com sua rotina e mantendo, sempre que possível, a mesma conexão. Dessa forma, cada conjunto de experimentos reflete condições reais de uso específicas de cada integrante.

3.1 Jitter

O jitter foi analisado a partir da variação do atraso (RTT) entre pacotes consecutivos, em milissegundos, ao longo do tempo. Em termos práticos, ele representa o quanto a latência oscila de um pacote para o outro: quanto maior o jitter, menos previsível é o atraso, o que pode prejudicar aplicações sensíveis a tempo real, como chamadas de vídeo, VoIP e jogos online.

Para visualizar esse comportamento, o jitter foi avaliado a partir do desempenho médio por hora, separando-se os cenários com VPN ligada e desligada para cada integrante do grupo. Os resultados apresentaram comportamentos distintos entre os membros. No caso de Gabriel, observou-se um aumento consistente do jitter quando a VPN estava desligada em praticamente todos os períodos analisados. Para Ester, o comportamento foi mais oscilatório, com alternância entre momentos em que a VPN ligada apresentava maior jitter e outros em que o cenário sem VPN era mais instável. Já para Júlia, os valores de jitter com e sem VPN permaneceram próximos ao longo do tempo, indicando que, no ambiente de teste dela, o uso da VPN não introduziu variações tão significativas nessa métrica.

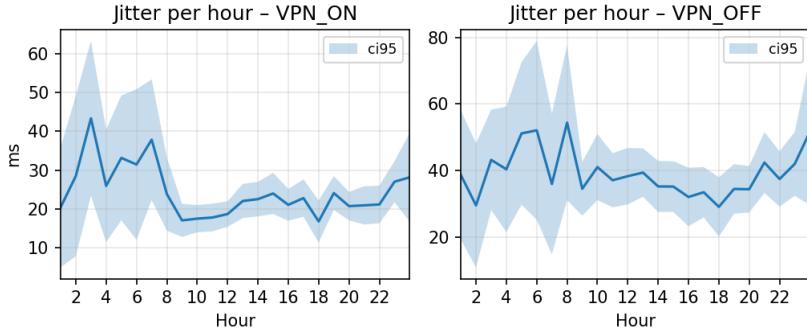


Fig. 1. Comparação de jitter com e sem VPN por hora para Gabriel

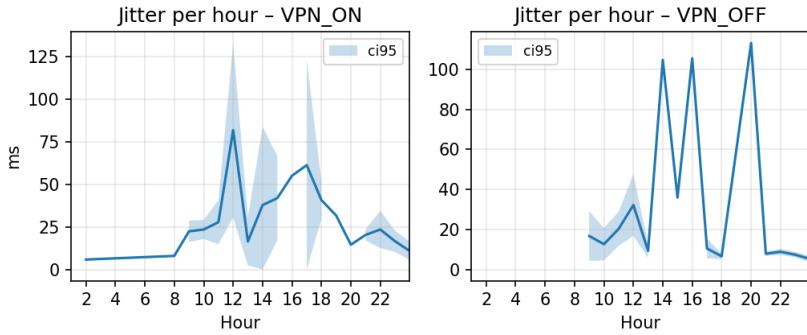


Fig. 2. Comparação de jitter com e sem VPN por hora para Ester

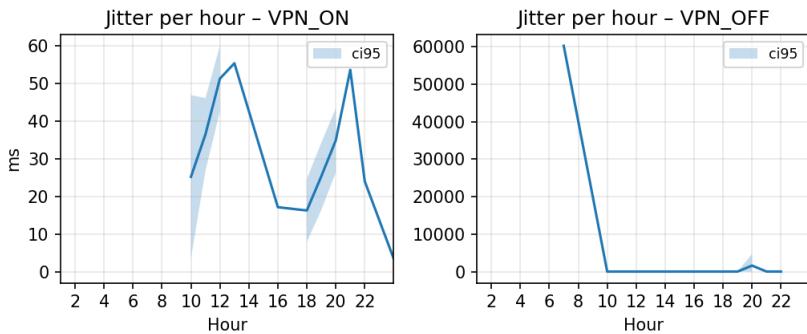


Fig. 3. Comparação de jitter com e sem VPN por hora para Julia

3.2 Latência

Para o estudo dos resultados obtidos a partir dos dados de latência, foi feita uma breve análise dessa métrica. A latência corresponde ao tempo que um pacote leva para sair da

máquina do usuário, alcançar o destino e retornar (RTT), sendo percebida como o “atraso” entre uma requisição e a resposta do sistema. Valores elevados de latência tendem a impactar negativamente aplicações interativas, como navegação web, acesso remoto e serviços em tempo quase real.

A análise da latência foi realizada a partir de sua variação ao longo das horas do dia, considerando separadamente os cenários com VPN ligada e desligada para cada integrante do grupo. Os resultados apresentaram diferenças significativas entre os membros, refletindo as particularidades de cada ambiente de rede. No entanto, destaca-se que, no caso dos experimentos realizados por Gabriel, a latência medida com a VPN desligada se manteve consistentemente mais alta do que com a VPN ativada, contrariando a hipótese inicial de que o uso da VPN sempre aumentaria o atraso. Esse comportamento sugere que fatores externos, como o roteamento adotado pelo provedor ou condições momentâneas da rede, também exercem influência relevante sobre a latência observada.

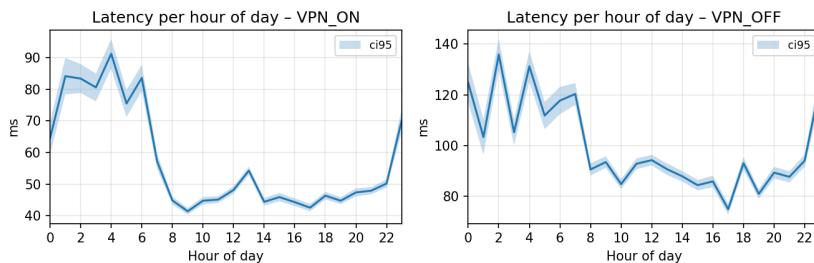


Fig. 4. Latência por hora para Gabriel

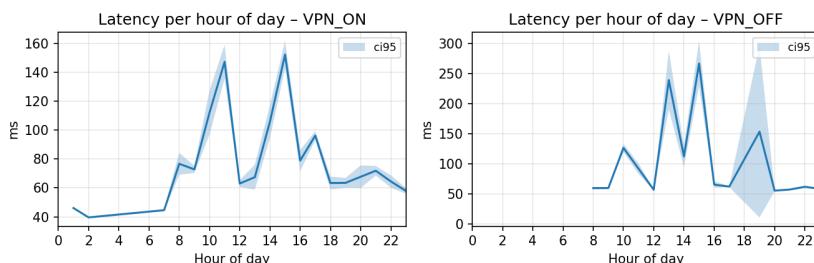


Fig. 5. Latência por hora para Ester

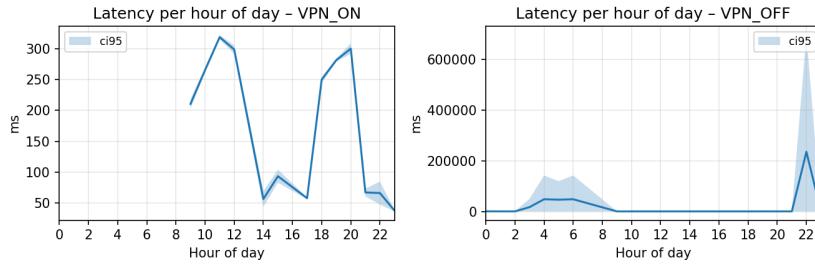


Fig. 6. Latência por hora para Julia

3.3 Perda de pacotes

Para a perda de pacotes, foi analisada a taxa percentual de pacotes perdidos ao longo do período observado. A perda de pacotes representa a proporção de mensagens enviadas que não chegam corretamente ao destino, seja por descarte em roteadores intermediários, estouro de filas, erros de transmissão ou outros problemas na rede. Em termos práticos, valores mais altos de perda tendem a degradar a experiência do usuário, causando travamentos em vídeos, cortes em chamadas de voz e aumento de retransmissões em protocolos confiáveis.

Como já mencionado, após sucessivas rodadas de experimentos, foi identificado que a forma de armazenamento das informações de loss estava impactando indiretamente os resultados, o que poderia comprometer a confiabilidade da análise. Por esse motivo, optou-se por considerar apenas os dados da primeira entrega do trabalho, na qual o processo de coleta e registro estava mais consistente.

A partir desses dados, observa-se que, para ambos os integrantes analisados, a perda de pacotes se mostra mais expressiva nos testes realizados com a VPN ativada, indicando uma influência direta do uso do túnel VPN sobre essa métrica. Em particular, nota-se um aumento da taxa de perda em relação ao cenário sem VPN, o que reforça a ideia de que a sobrecarga introduzida pela VPN pode agravar problemas de descarte de pacotes em situações de maior carga ou variação de qualidade da conexão.

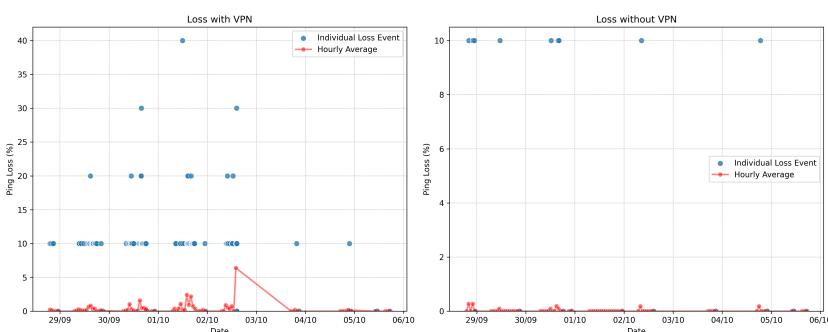


Fig. 7. Comparação de perda de pacotes com e sem VPN para Gabriel

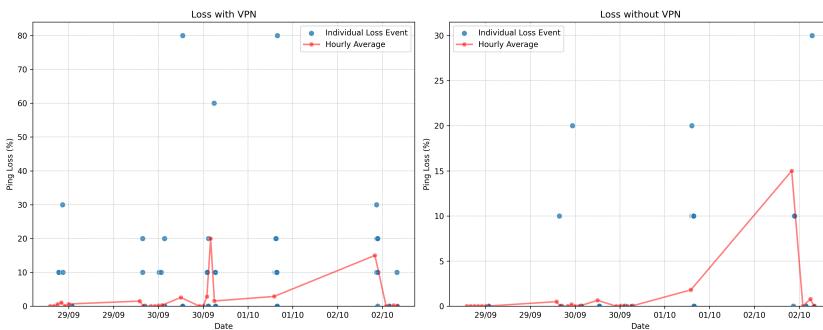


Fig. 8. Comparação de perda de pacotes com e sem VPN para Ester

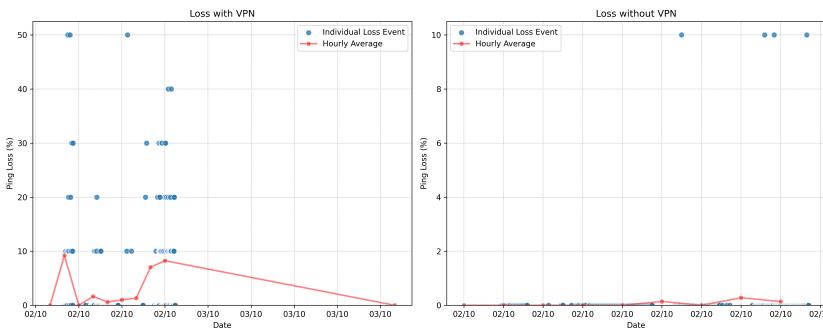


Fig. 9. Comparação de perda de pacotes com e sem VPN para Julia

3.4 Vazão

Para a vazão, foram analisados os valores médios de taxa de transmissão obtidos pelo iperf ao longo do período de coleta, tanto com a VPN ativada quanto desativada. A vazão (throughput) representa a quantidade de dados efetivamente transmitidos por unidade de tempo entre cliente e servidor, estando diretamente relacionada à rapidez percebida em atividades como download de arquivos, navegação em páginas web e uso de serviços de streaming.

Os resultados foram apresentados em gráficos separados para upload e download, permitindo comparar, para cada integrante do grupo, o comportamento da conexão com e sem o uso da VPN.

A partir dos dados observados, verificou-se que, em todos os casos, a ativação da VPN compromete o desempenho de vazão, resultando, na maioria das amostras, em taxas significativamente menores em comparação ao cenário sem VPN. Embora existam diferenças entre os resultados de cada participante, decorrentes das particularidades de cada ambiente de teste, o padrão geral aponta de forma consistente para a influência negativa da VPN sobre a vazão. Além disso, nota-se que, à medida que se aumentam o número de rodadas e o tempo total de experimento, essa diferença de desempenho entre os cenários com e sem VPN tende a se tornar ainda mais evidente.

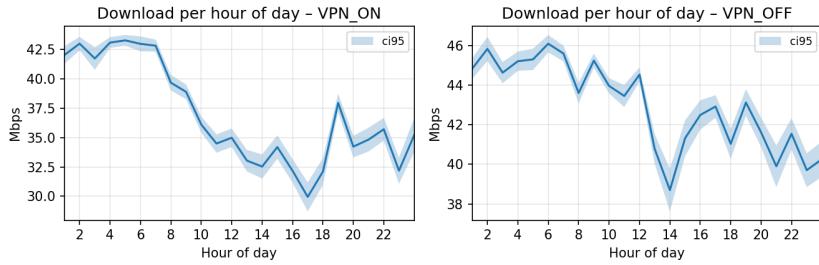


Fig. 10. Comparação da vazão para dowload com e sem VPN para Gabriel.

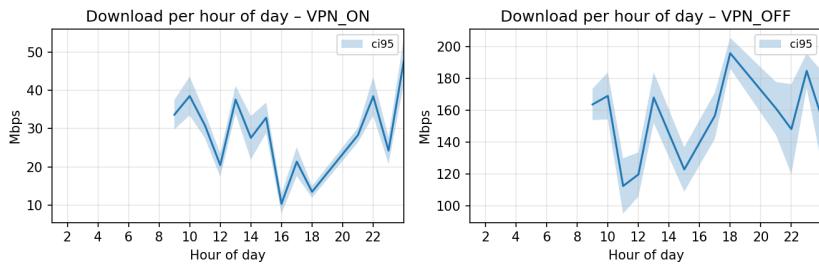


Fig. 11. Comparação da vazão para dowload com e sem VPN para Ester.

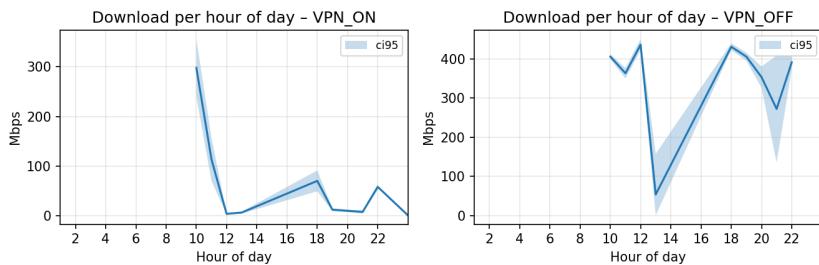


Fig. 12. Comparação da vazão para dowload com e sem VPN para Julia.

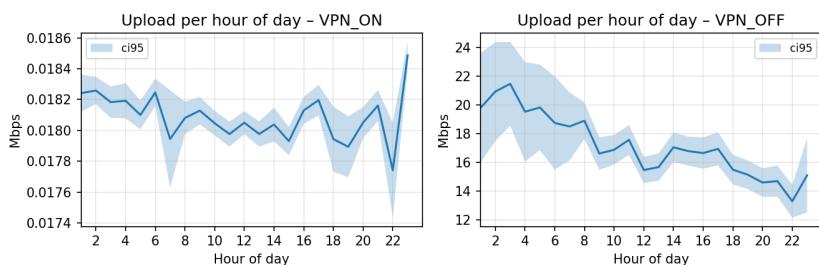


Fig. 13. Comparação da vazão para upload com e sem VPN para Gabriel.

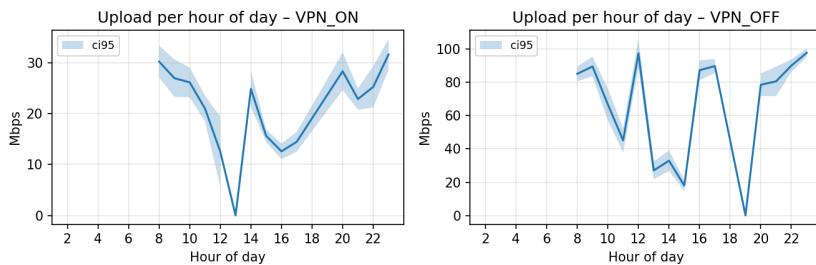


Fig. 14. Comparação da vazão para upload com e sem VPN para Ester.

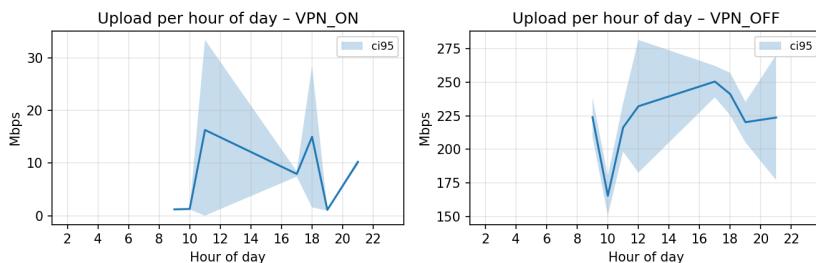


Fig. 15. Comparação da vazão para upload com e sem VPN para Julia.

4 CONCLUSÃO

A partir dos resultados apresentados na seção anterior, é possível concluir que a utilização da VPN da UFRGS de fato impacta o desempenho da conexão. Em termos de vazão, observou-se que, na maior parte dos casos, o uso da VPN resultou em pior desempenho tanto para download quanto para upload, reforçando a hipótese de que o túnel VPN introduz overhead e reduz a taxa efetiva de transmissão de dados.

No que diz respeito à perda de pacotes, os dados indicam que seriam necessários mais experimentos e uma coleta mais robusta para permitir conclusões definitivas. Como discutido em Resultados, alterações posteriores no script e na forma de armazenamento dos dados afetaram indiretamente esse indicador, motivo pelo qual as análises de loss foram baseadas principalmente na Etapa 2. Ainda assim, os resultados considerados apontam que a VPN ligada tende a agravar a perda de pacotes em relação ao cenário sem VPN.

Para jitter e latência, verificou-se um comportamento heterogêneo entre os integrantes do grupo e entre diferentes execuções, influenciado também pelas particularidades de ambiente de cada participante (como a troca de máquina no caso de Ester e diferenças de horários e condições de rede). Mesmo assim, à medida que o número de rodadas de experimentos aumenta, torna-se mais evidente a influência da VPN no aumento da variabilidade do atraso e do tempo de resposta.

Dessa forma, considera-se que o objetivo do trabalho foi alcançado: foi possível aplicar, em um cenário real, os conceitos estudados na disciplina de Avaliação de Desempenho, compreender melhor o impacto prático do uso de VPN sobre diversas métricas de rede e exercitar o planejamento, a execução e a análise de experimentos de desempenho de forma estruturada.

5 REFERÊNCIAS

REFERENCES

- [1] Raj Jain. *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*. John Wiley & Sons, New York, 1991. ISBN 0471503363.
- [2] Douglas C. Montgomery and George C. Runger. *Applied Statistics and Probability for Engineers*. 6th edition, Wiley.
- [3] H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson. *RTP: A Transport Protocol for Real-Time Applications*. RFC 3550 (Standard), 2003. Disponível em: <https://www.rfc-editor.org/rfc/rfc3550>. Acesso em: 30 nov. 2025.
- [4] Jean-Yves Le Boudec. *Performance Evaluation Of Computer And Communication Systems*. 2010. ISBN 978-2-940222-40-7. Disponível em: <https://leboudec.github.io/perfeval/>. Acesso em: 30 nov. 2025.
- [5] Nicolas P. Rougier, Michael Droettboom and Philip E. Bourne. Ten simple rules for better figures. *PLOS Computational Biology*, 10(9):e1003833, 2014. DOI: 10.1371/journal.pcbi.1003833. Disponível em: <https://doi.org/10.1371/journal.pcbi.1003833>. Acesso em: 30 nov. 2025.