Lab-Redes T1 - Monitoramento de Tráfego em Túnel
Brenda Pereira Camara, João Pedro Salles da Silva, Leonardo Bertoletti

1. Introdução

Este relatório descreve o desenvolvimento e uso de um sistema para monitoramento de tráfego de rede em ambientes virtualizados, utilizando Java e C. O sistema permite criar um túnel de rede entre dois dispositivos (cliente e servidor) e monitorar, em tempo real, os pacotes que trafegam por esse túnel, registrando informações detalhadas em arquivos CSV para análise posterior.

2. Estrutura Geral do Sistema

O sistema é composto por dois principais componentes:

Túnel de Rede (traffic_tunnel):

Implementado em C, cria uma interface virtual (tun0) em cada máquina, conectando cliente e servidor. O tráfego enviado para tun0 em uma ponta é transmitido para a outra ponta, simulando uma VPN ponto-a-ponto.

Monitor de Tráfego (Java):

Um programa em Java que utiliza a biblioteca Pcap4J para capturar pacotes em tempo real de qualquer interface de rede (física ou virtual). O monitor exibe estatísticas na tela e salva detalhes dos pacotes em arquivos CSV, separados por camada (enlace, rede e transporte).

3. Requisitos e Evidências de Implementação

Criação e uso do túnel de rede:

O túnel é iniciado com comandos específicos em cada máquina, usando os IPs corretos das interfaces físicas.

Exemplo de comando no cliente:

./traffic_tunnel eth0 -c 172.31.66.2 -t ./client1.sh &

Exemplo de comando no servidor:

./traffic_tunnel eth0 -s 172.31.66.1 -t ./server.sh &

Após a configuração, cada máquina possui uma interface tun0 ativa.

Monitoramento do tráfego

O monitor é executado com o comando:

java -jar target/network-monitor-1.0.0.jar tun0

Ele exibe estatísticas como número de pacotes, bytes e protocolos detectados.

Os dados são salvos em arquivos CSV (camada2.csv, camada3.csv, camada4.csv).

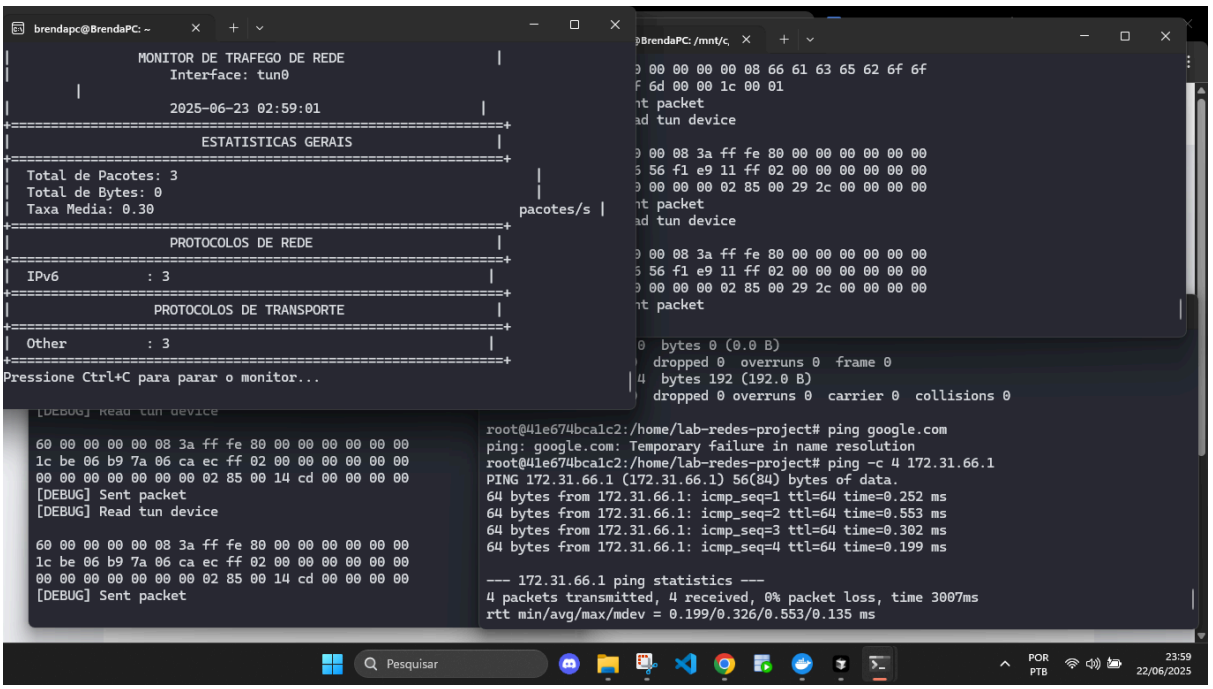
Geração e captura de tráfego

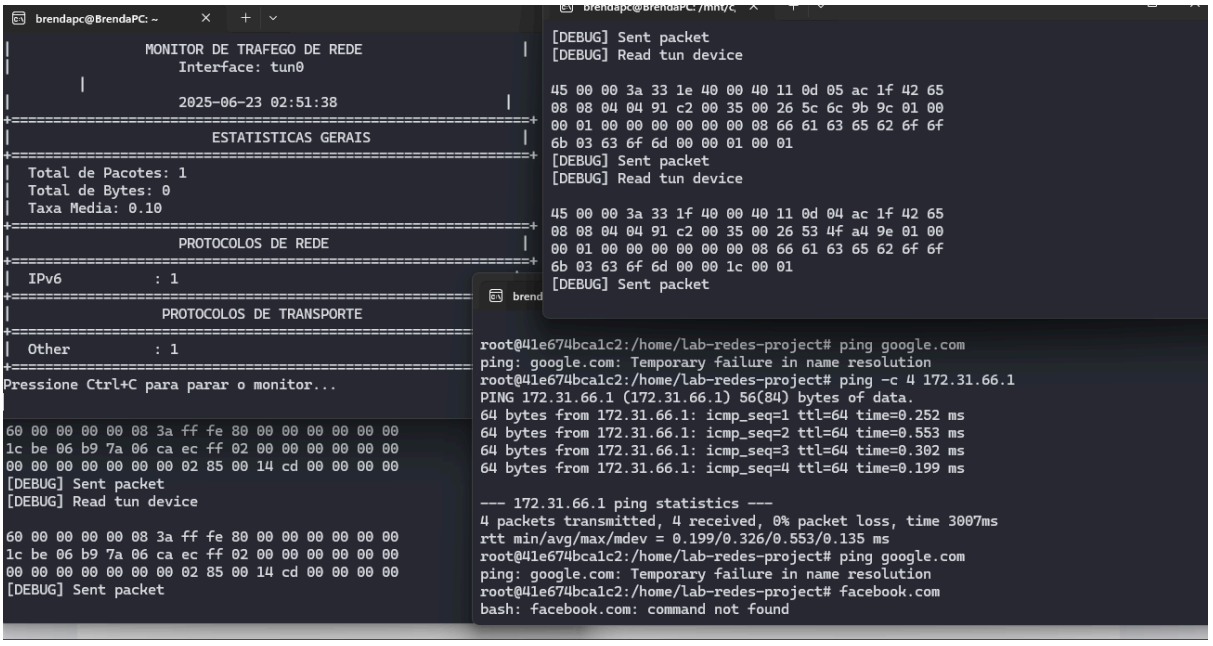
Para testar, comandos como ping são usados para gerar tráfego entre as interfaces tun0 dos dois lados. O monitor registra o tráfego gerado, comprovando o funcionamento do sistema.

Evidências

Os arquivos CSV mostram os pacotes capturados, com informações como endereços IP, portas, protocolos e tamanhos.

O monitor exibe em tempo real o aumento dos contadores de pacotes e bytes ao gerar tráfego pelo túnel.





4. Considerações Finais

O sistema desenvolvido permitiu criar um ambiente de rede virtualizado, onde foi possível monitorar detalhadamente o tráfego que passa por um túnel VPN customizado. Aprendemos a importância de configurar corretamente os IPs e interfaces para que o tráfego realmente passe pelo túnel, além de entender como funciona a captura de pacotes em diferentes camadas da rede. O uso de arquivos CSV facilitou a análise dos dados coletados. Enfrentamos desafios como garantir que o binário do túnel não estivesse travado e que o tráfego realmente passasse pela interface tun0, mas conseguimos superar esses obstáculos com testes e ajustes nos comandos. O trabalho foi fundamental para consolidar conhecimentos sobre tunelamento, monitoramento e análise de tráfego em redes.