ANALYSIS OF IP VPN PERFORMANCE

ENSC 427: Communication Networks, Spring 2012

Group 12 Final Project

Faiz Parkar, 301044177 (fkp@sfu.ca)
Kevin Chung Hang Wong, 301072117 (kcw6@sfu.ca)

http://www.sfu.ca/~fkp/Index.html

Roadmap

- Introduction
- Background Information
- Motivation
- Network Model
- Scenarios
- Simulation Results
- Conclusion
- Future Work
- References

Introduction

- Project models a site-to-site VPN network
- We analyze the performance of some commonly used applications (in an office environment) such as email, FTP and remote log-in over a firewall-protected IP VPN connection
- OPNET used to simulate basic and expanded scenarios

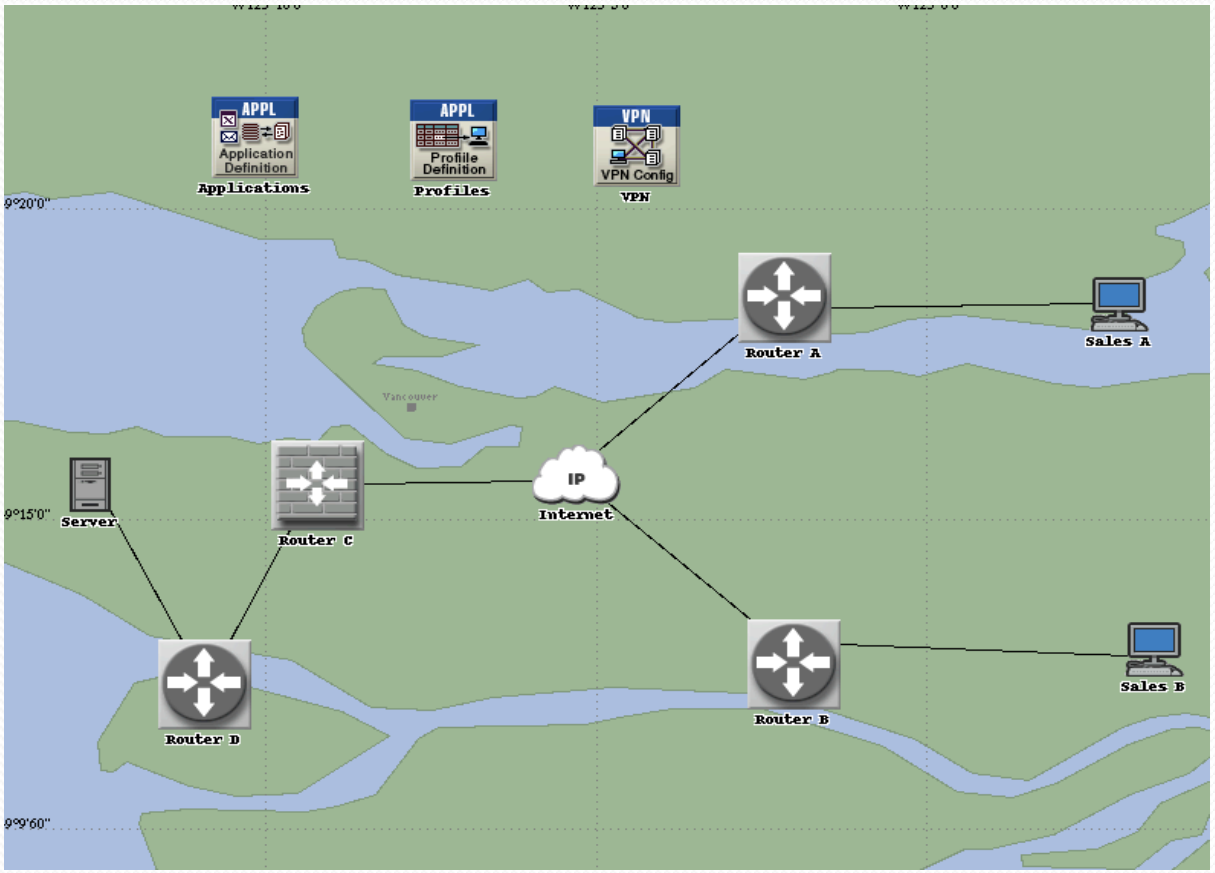
Background Information

- Virtual Private Network (VPN) allows remote users to connect to a central organizational network using public telecommunication infrastructure, such as the Internet
- Data being transferred through the VPN tunnel is secured using various encryption technologies
- No need to build dedicated leased lines to connect remote users to a private network

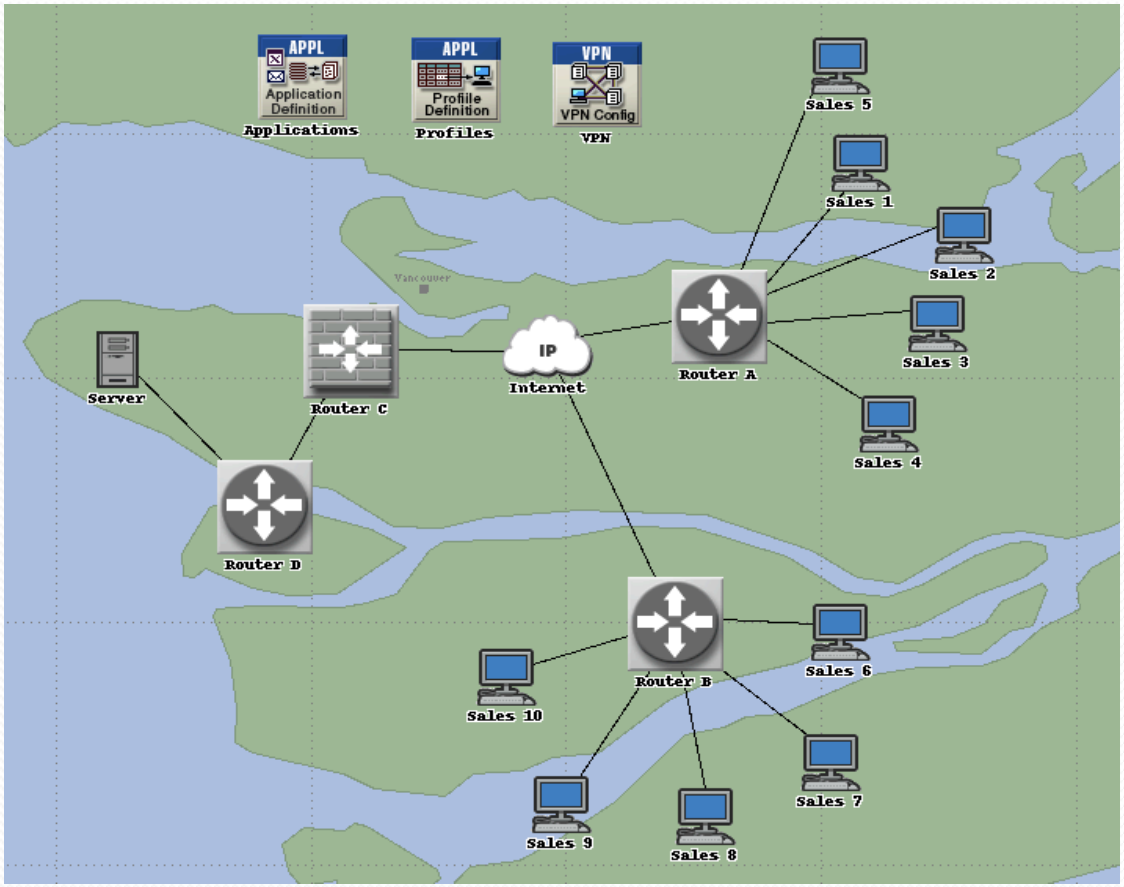
Motivation

- Analyze the application server's Quality of Service
- Observe VPN tunnel performance due to increase in traffic
- Explore types of network expansions supported under the IP VPN configuration in OPNET
- Get a better understanding of what parameters can be modified under secure site-to-site VPN networks

Network Topology (Baseline)



Network Topology (Expanded)

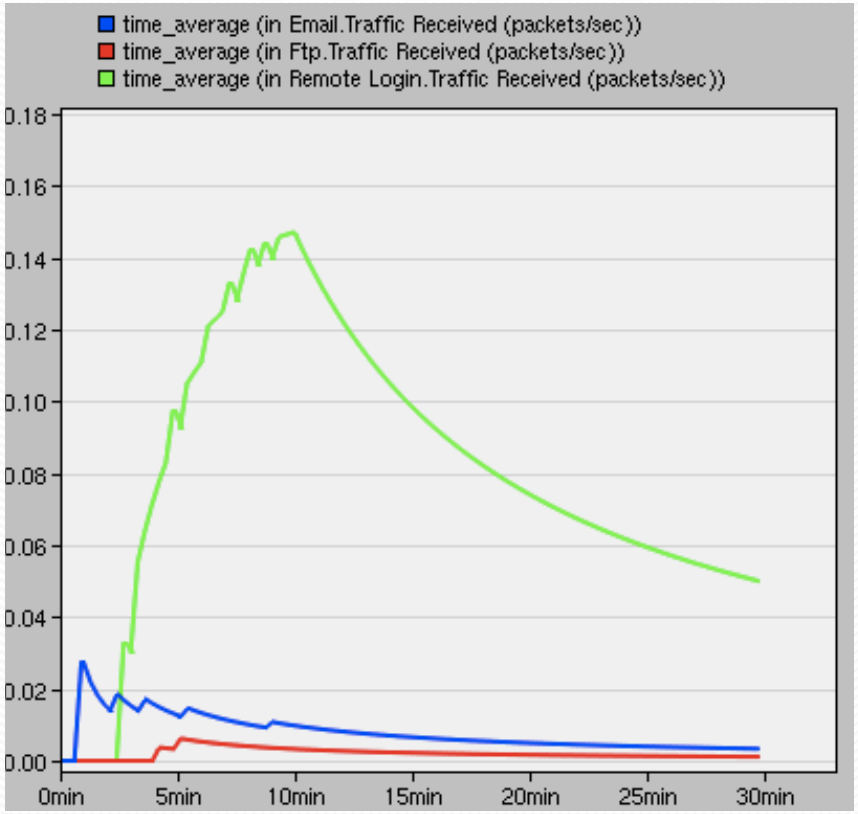


Scenarios

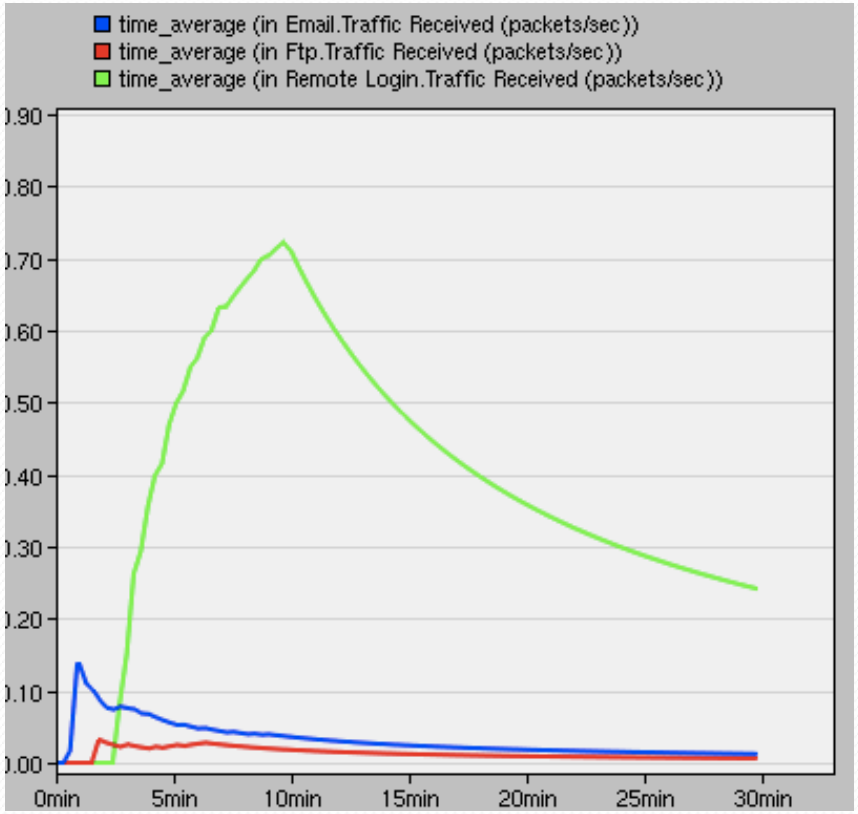
- Workstations will attempt to access applications on the server through site-to-site VPN tunnelling
- Applications: Heavy Email, FTP, and remote login
- Scenarios:
  1. 2 workstations connecting to an Internet cloud through 2 different routers, which connects to the server through a firewall and final router connected to the server
  2. Expansion of above network with 5 workstations on each router

Simulation Results

Baseline Network

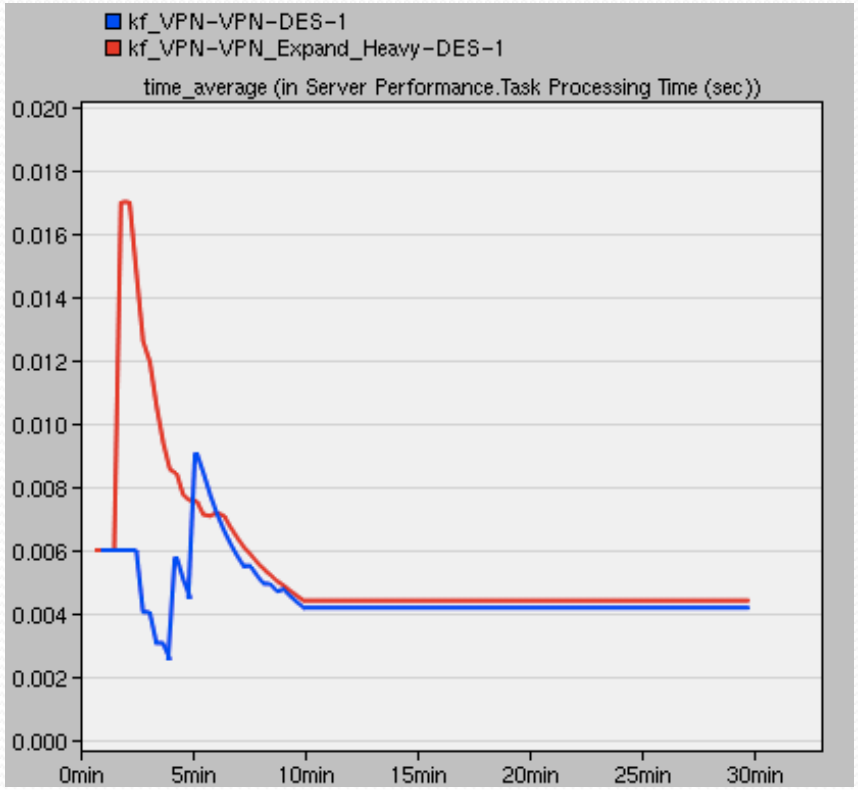


Expanded Network

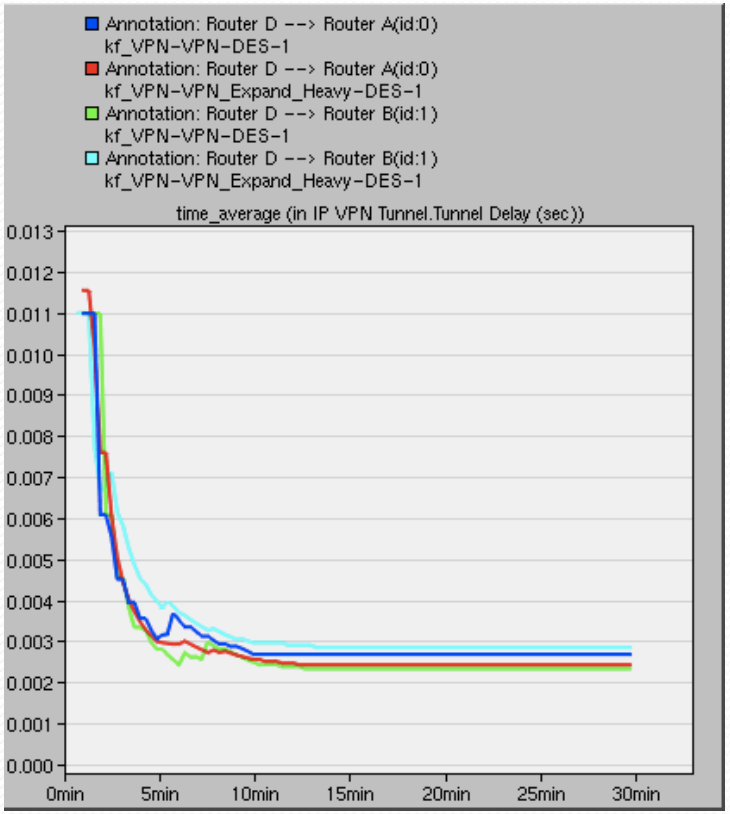


Simulation Results

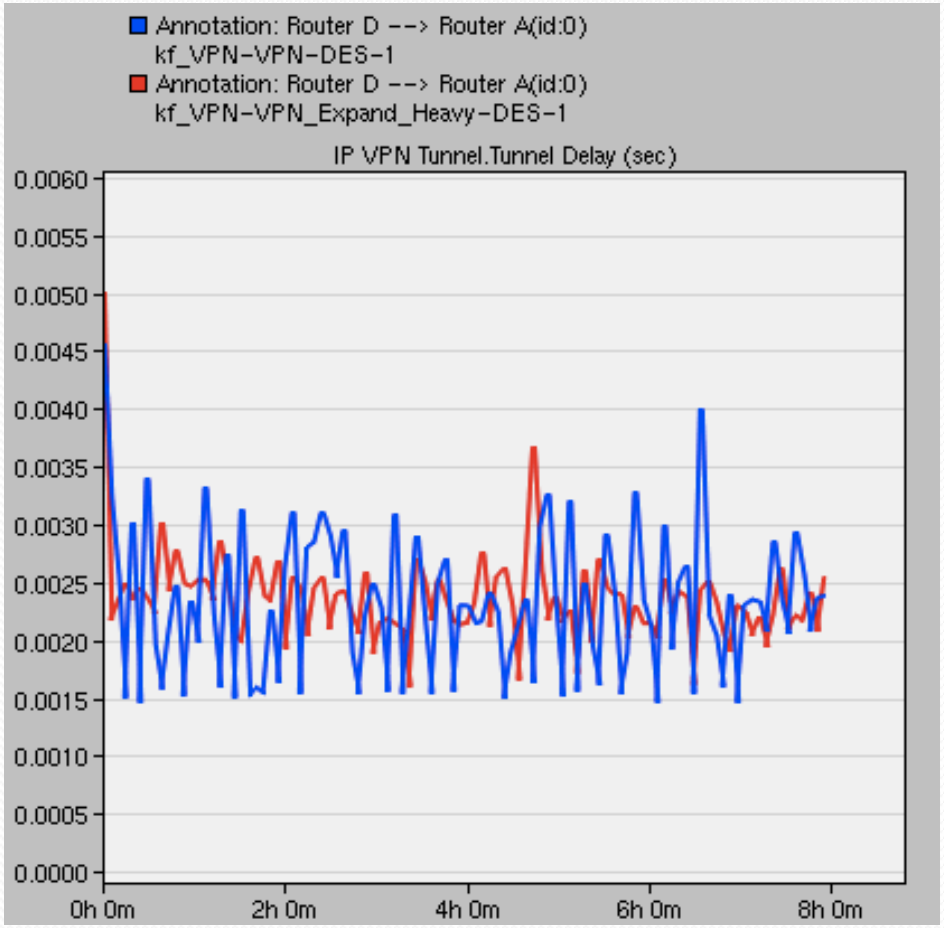
Server Processing Time



IP VPN Tunnel Delay



Simulation Results (8 hours)



Conclusion

- IP VPN Tunnel delay-curves similar in both scenarios
- Increase in traffic affects server performance greater than the VPN tunnel delay
- Current model unable to support more than two routers with client workstations connecting to the Internet
- Difficulties in finding the relevant statistics

Future Work

- Expand the network even further by adding more workstations
- Work with MPLS VPN to compare performance with additional routers and multi-office networks
- Model Video-Conferencing correctly between internal and remote workstations

References

- [1] A. Zaballos, G. Corral, I. Serra, J. Abella, "Testing Network Security Using OPNET," OPNETWORK.2003, Washington DC (United States), August 2003.
- [2] E. Aboelela, "Firewalls and VPN: Network Security and Virtual Private Networks," Computer Networks: A Systems Approach - Network Simulation Experiments Manual, 5ed, March 2011.
- [3] H. Bourdoucen, A. Al Naamany, A. Al Kalbani, "Impact of Implementing VPN to Secure Wireless LAN," International Journal of Computer and Information Engineering, 2009.
- [4] R. Malhotra, R. Narula, "Techno-Evaluation and Empirical Study of Virtual Private Networks Using Simulations," Journal of Computing, Volume 3, Issue 7, July 2011.
- [5] Matutes Mestre, Manuel, "Simulation-Based Analysis of VPN Technologies," 2003.

Questions?