SFU

Spring 2012

ENSC 427: Communication Networks

Creating a Secure Network through Firewalls and Virtual Private Networks

http://www.sfu.ca/~msa102

Team #2

Maxim Soleimani-Nouri	msa102@sfu.ca	301103660
Andy Cheng	alc21@sfu.ca	301090416
Saman Mehdizadeh	sas20@sfu.ca	301092517

Roadmap

- Motivation
- Background Information
- OPNET Simulation
- Results & Discussion
- Related Works
- Future Works
- Conclusion
- References

Roadmap

- Motivation
- Background Information
- OPNET Simulation
- Results & Discussion
- Related Works
- Future Works
- Conclusion
- References

Motivation

- Why bother with security?
- These services connect to the internet.
- Internet has evolved into a place ridden with viruses, spyware, and malicious users.
- What forms of security are available?

Roadmap

- Motivation
- Background Information
- OPNET Simulation
- Results & Discussion
- Related Works
- Future Works
- Conclusion
- References

What is a Firewall?

- DEFINITION: A device used to regulate traffic by enforcing specific policies

- Three main types:
  - Packet filtering
  - Network (or stateful packet inspection)
  - Application

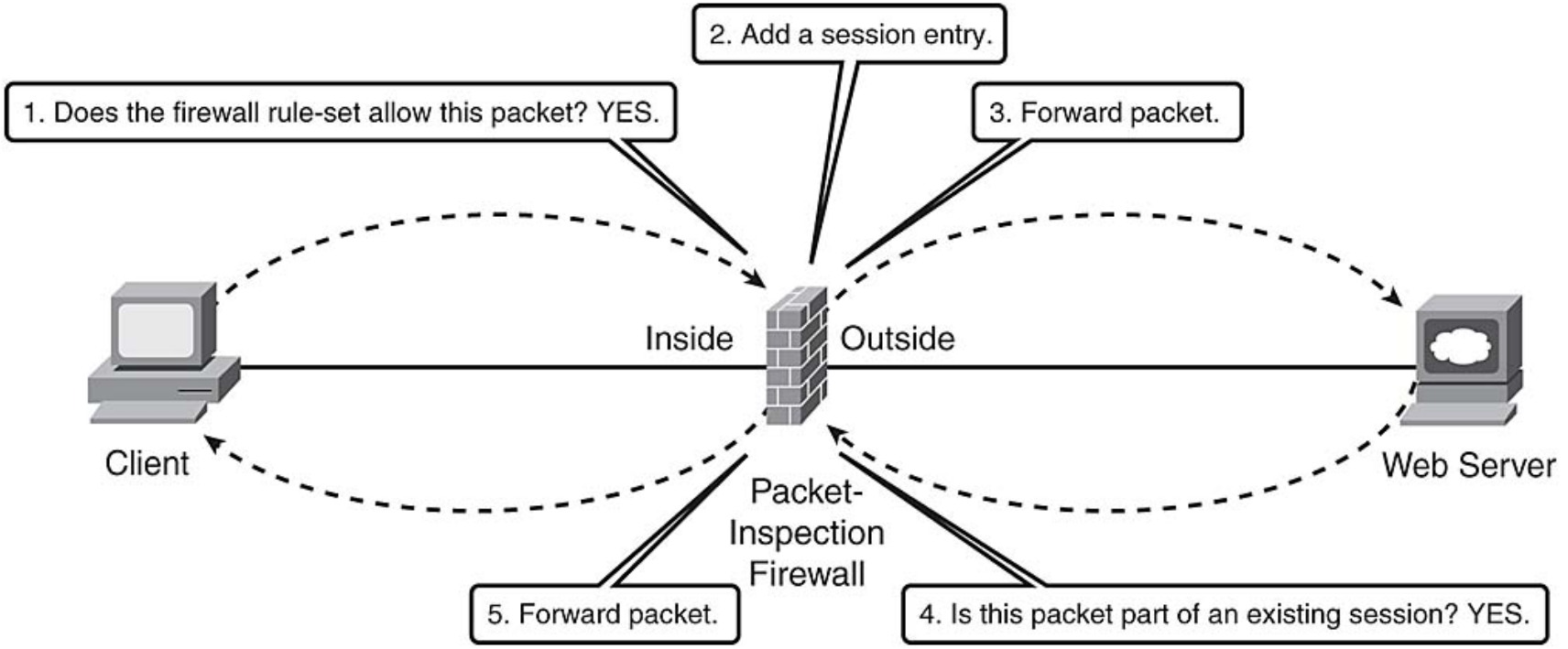
Packet Filtering Firewall

- Began in 1988 as a “Packet Filter”
- Looks at IP header of packet containing the protocol (TCP/UDP), source/destination and port number
- Block certain applications (http, ftp, telnet, etc.) by blocking a specific port.
- Ex. Select TCP and port 23 to block telnet access
- Advantages: most devices on your network have it, easy to implement for fast security
- Disadvantages: cannot look into the payload

Stateful inspection Firewalls

- 1989-1990 emergence of “stateful” filters, or inspection
- Looks at the session information such as protocol, new or existing connection and source and destination port numbers.
- Ability to inspect the payload if it matches the protocol (if HTTP connection, it checks if the content is legitimate HTTP data)
- Advantage: very fast (compared to application firewalls)

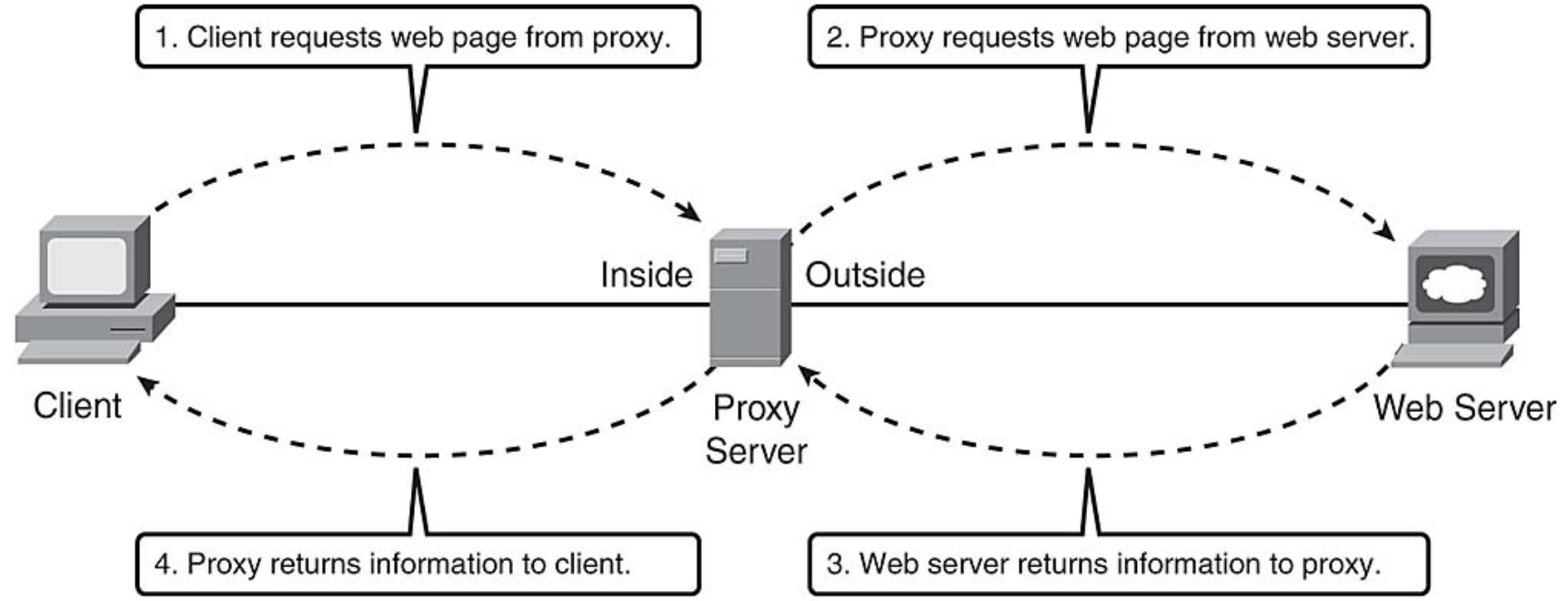
How Packet-Inspections Works



Application/Proxy Firewall

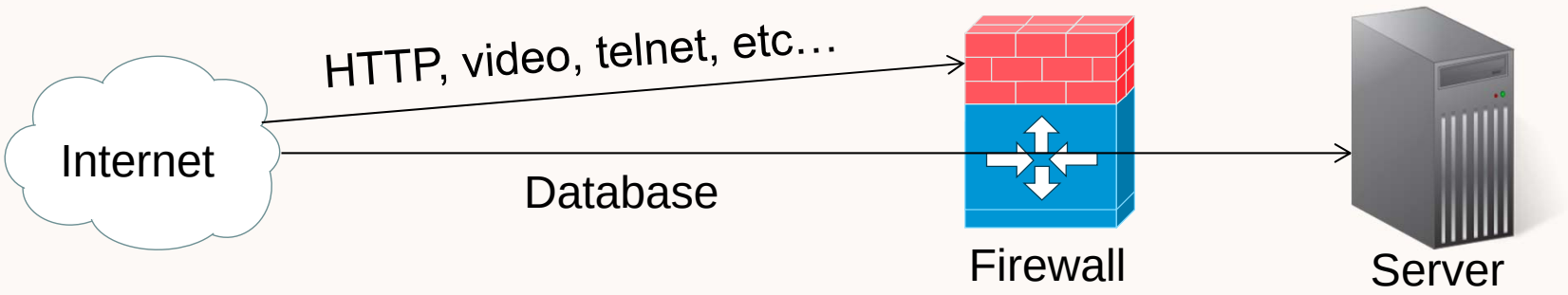
- Operates at layer 7 of the OSI model (application layer)
- The firewall or proxy acts as a mediator between client and IP service
- Advantages: acts on behalf of client, protects against port scans and application attacks
- Disadvantages: much slower than packet filtering and inspection (must host the application)

How Proxies Work



The Modern Firewall

Ex : Allow firewall to permit only database traffic to flow in and/or out of the server



Virtual Private Networks

- We now know how to protect our network from unauthorized access
- How do you remotely access network services?
- Create a logical private “tunnel” between two routers over the internet, or **Virtual Private Network** (VPN)
- No need for physical connection
- Remote user can access anything on the protected network regardless of firewall

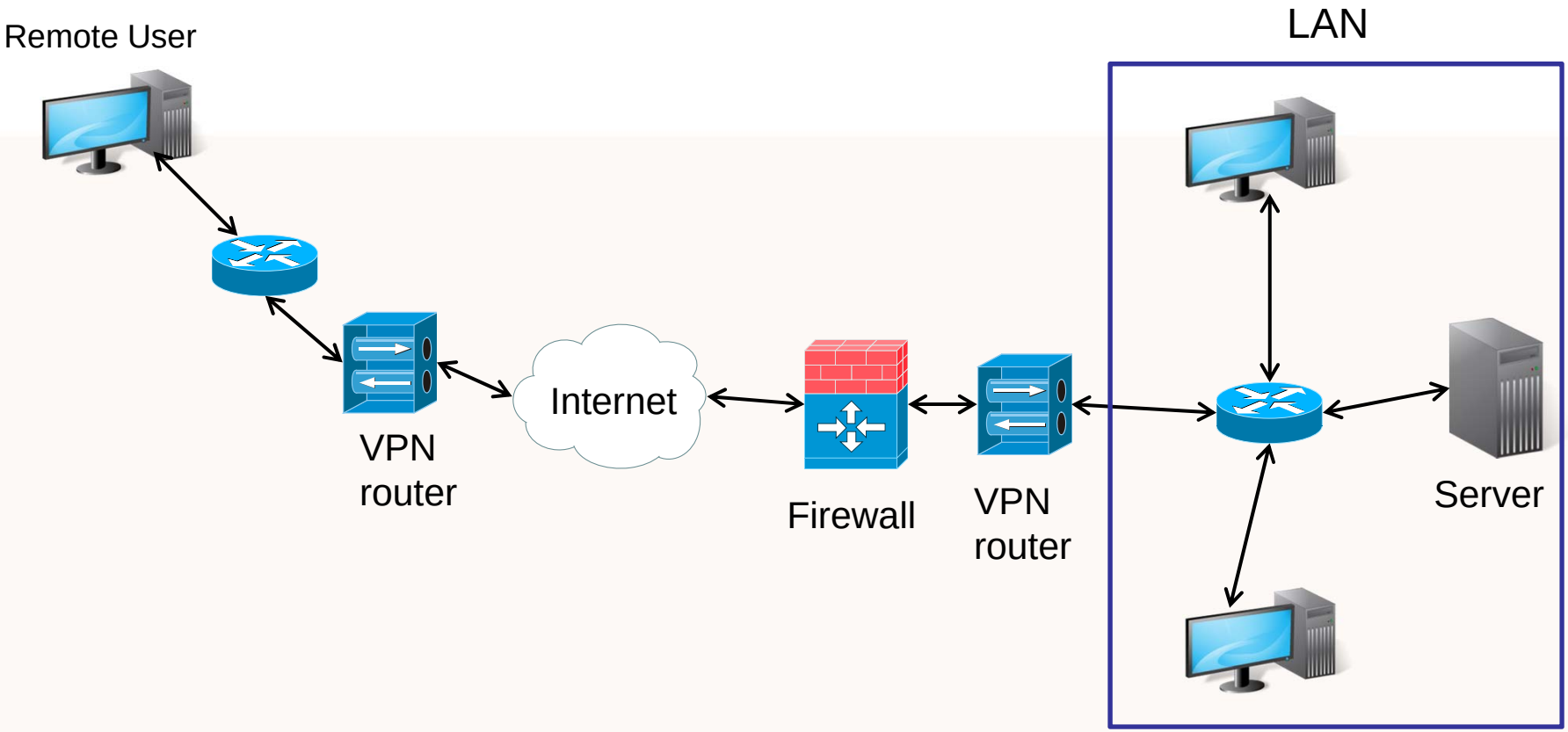
Types of VPNs

- Two types of VPNs
  - Voluntary
  - Compulsory
- Voluntary: client initiates connection with VPN server
- Compulsory: connection created between two VPN servers or routers
- Compulsory connections are done through either LAN or the internet
- Tunnels can be created at layer 2 and 3 of the OSI (data-link and network)

VPN Example

- Remote user trying to access services on the server located on a local area network
- VPN router is placed between the LAN and firewall creating a “tunnel”
- User sees “direct connection” to the server and the services that are offered by it
- Remote user can also access peripherals such as printers located inside the LAN through applications such as Telnet

Virtual Private Networks



SFU

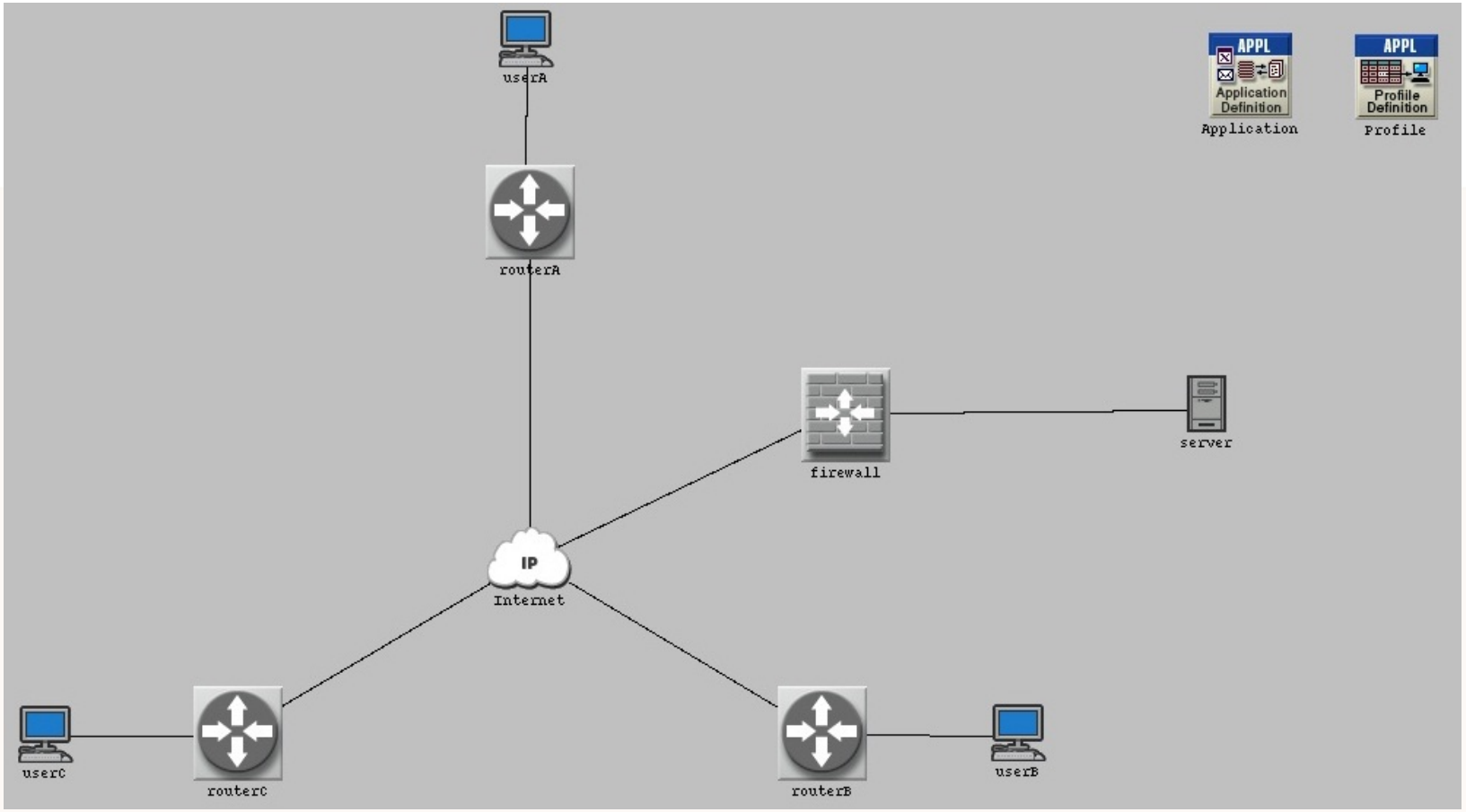
Roadmap

- Motivation
- Background Information
- OPNET Simulation
- Results & Discussion
- Related Works
- Future Works
- Conclusion
- References

Firewall Scenario

- Application configuration is used to set which services are used in this project
- Profile configuration is used to set the applications accessible by the users
- 3 users(A,B,C) are connected through IP cloud
- Server is set to offer all services but is protected by the firewall
- Users A, B, and C are set to request HTTP & Database services
- Firewall is set to deny access to the Database

Firewall Scenario

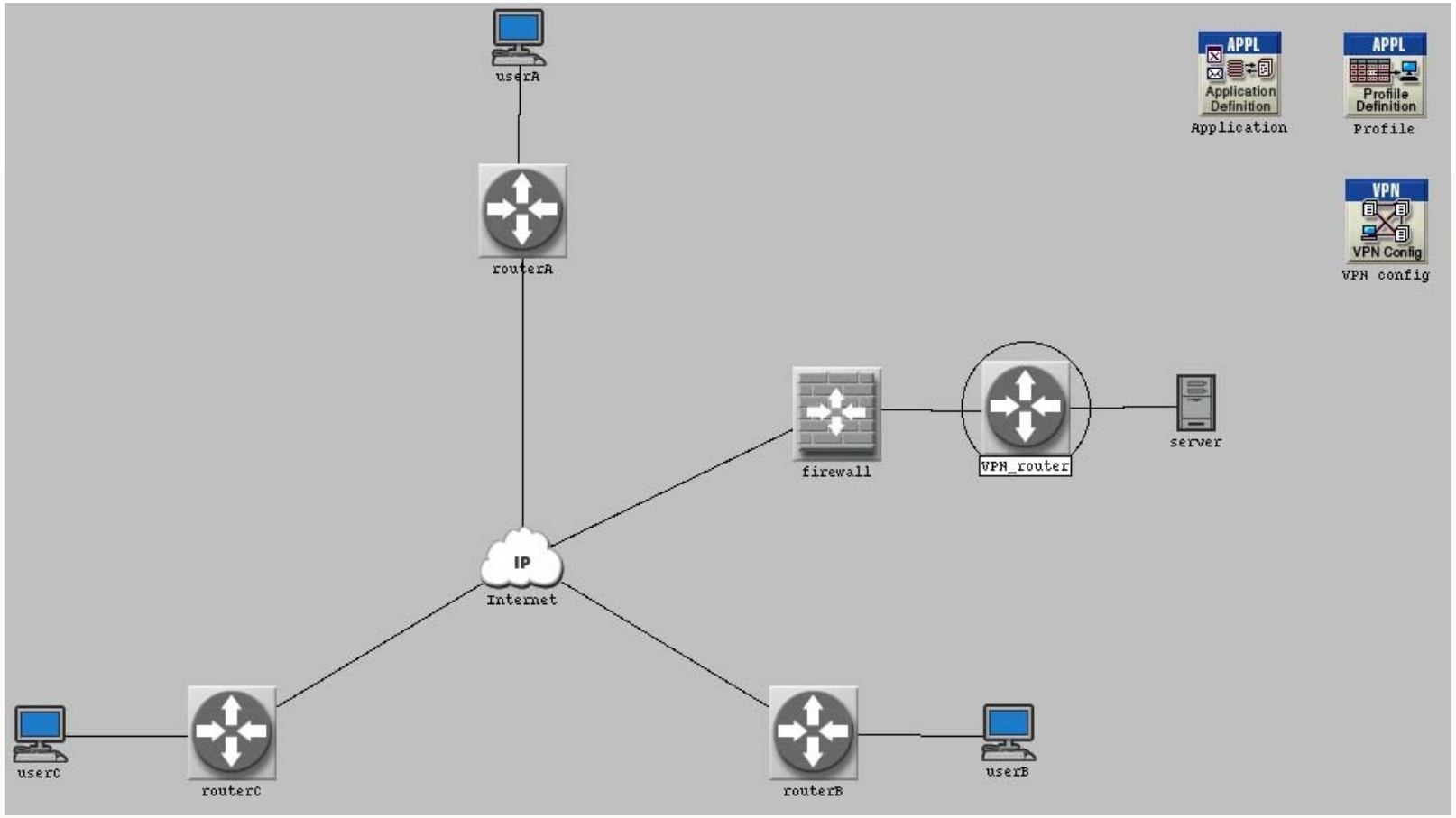


SFU

Firewall and VPN Scenario

- VPN router is placed between the firewall and the server
- VPN configuration is set to create a “tunnel” between router A and the VPN router granting user A services offered by the server

Firewall and VPN Scenario

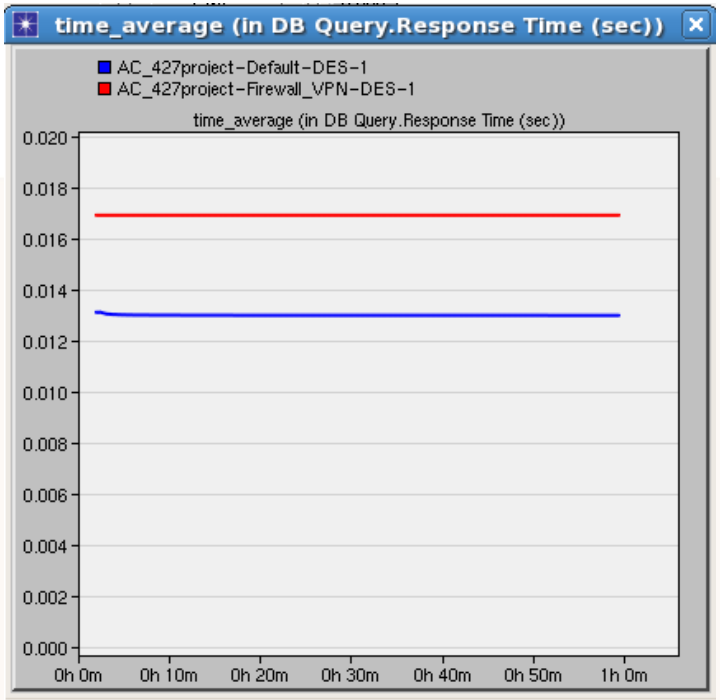


SFU

Roadmap

- Motivation
- Implementation
- OPNET Simulation
- Results & Discussion
- Related Works
- Future Works
- Conclusion
- References

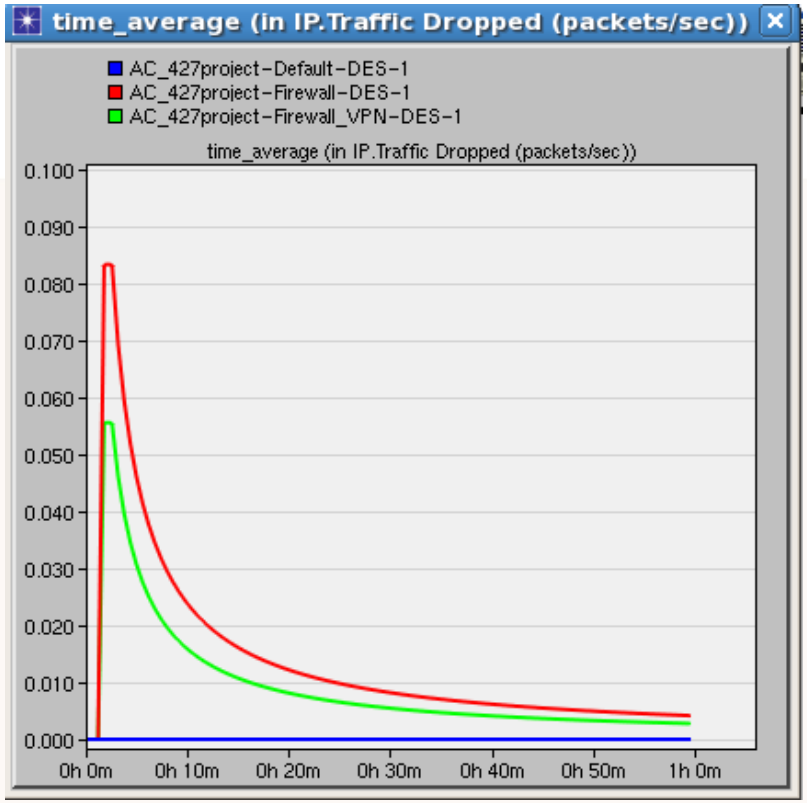
Results and Discussion



Database Query Response time

- Response time for DB Queries is higher on networks with firewalls and VPNs.
- VPN networks introduced a little more delay as opposed to the firewall.

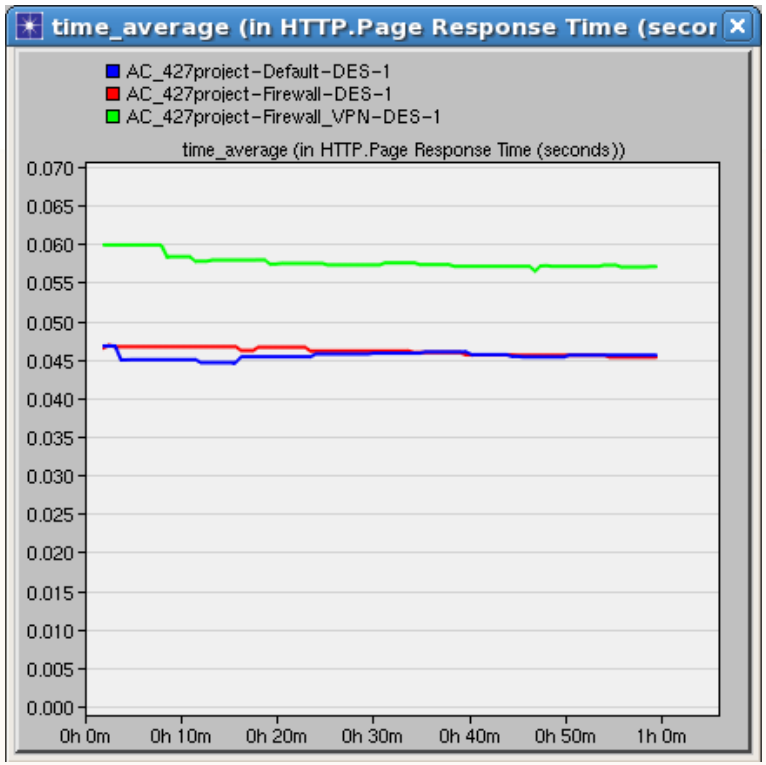
Results and Discussion



# of packets dropped per second

- In default scenario, no packets were dropped globally
- Introducing a firewall caused a spike in packets dropped due to the blocking of DB access(red)
- When routerA was tunneled to VPN_router, a Virtual Private Network was established, granting access to userA
- This can be seen in the reduction of packet drops for the VPN scenario(green)

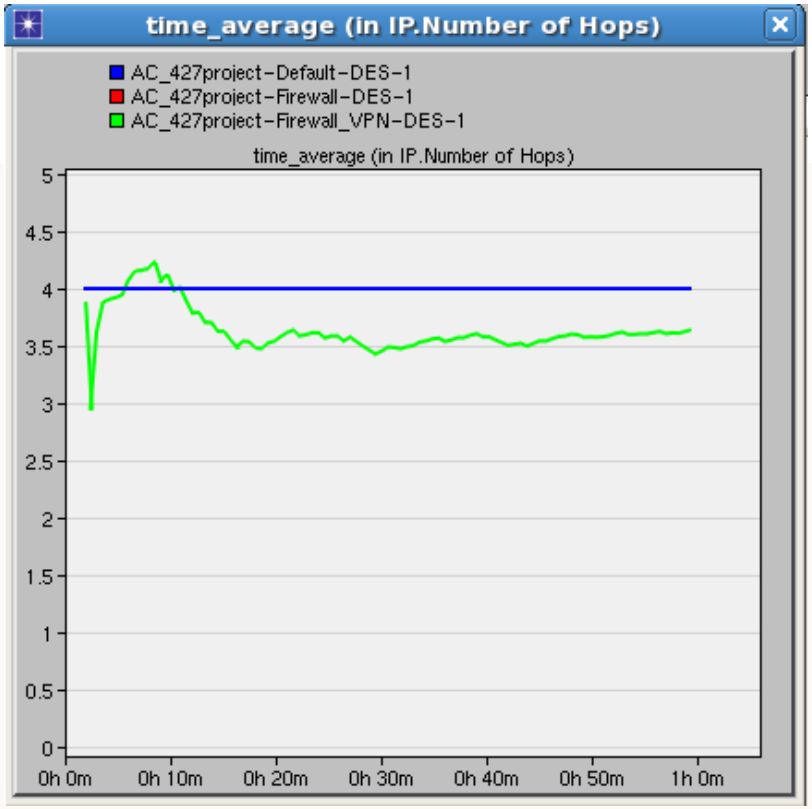
Results and Discussion



Page response time (HTTP)

- In the case of the HTTP application, the response time was roughly the same for the default and firewall scenario
- In the VPN scenario, a slight delay was introduced.

Results and Discussion

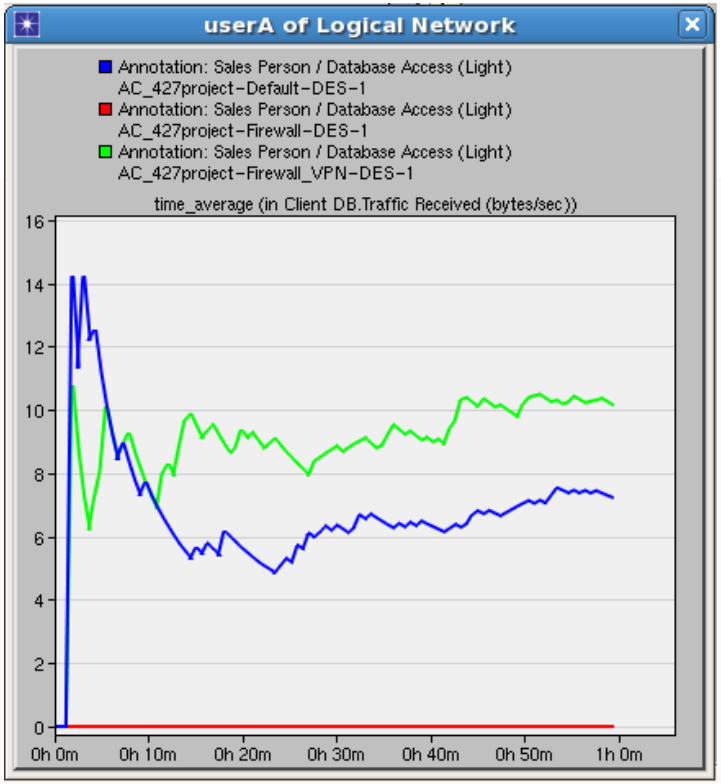


# of hops

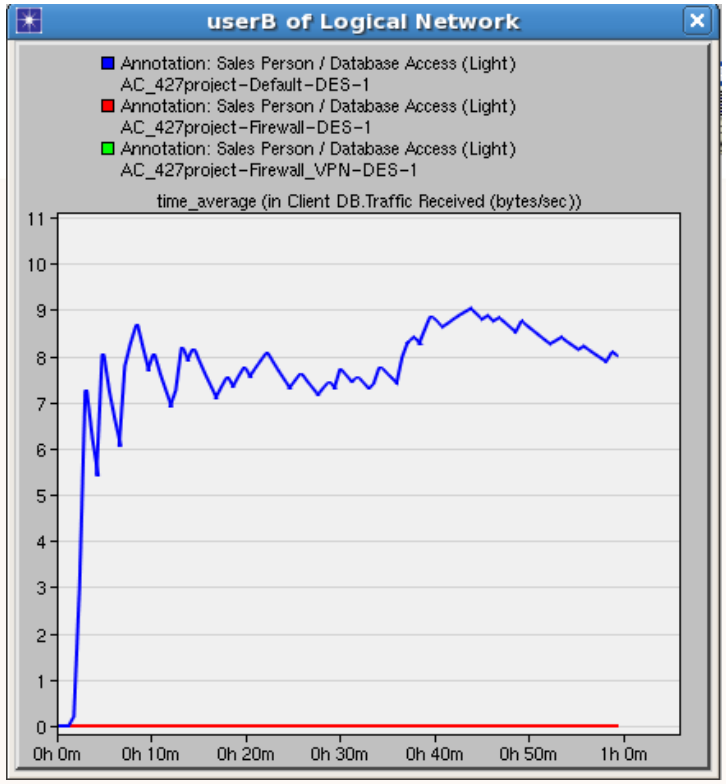
- Here we look at the number of “hops” made
- A Hop is simply a distance between two network devices in a network
- For the firewall scenario, the packet must first hop from userA to routerA, then to the IP cloud, then to the firewall, and finally to the server making a total of 4 hops as seen on the graph
- VPN introduces less hops on average since it creates a virtual gateway directly between userA and VPN_router

Results and Discussion

Comparing userA and userB for Database traffic received



userA Traffic Received for Database



userB Traffic Received for Database

SFU

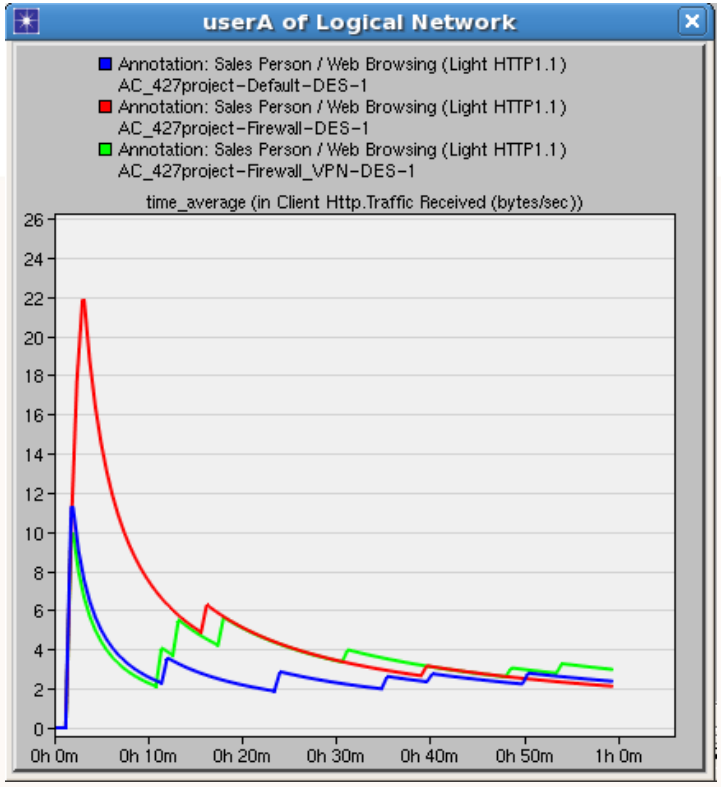
Results and Discussion

Comparison of traffic statistics between userA and userB

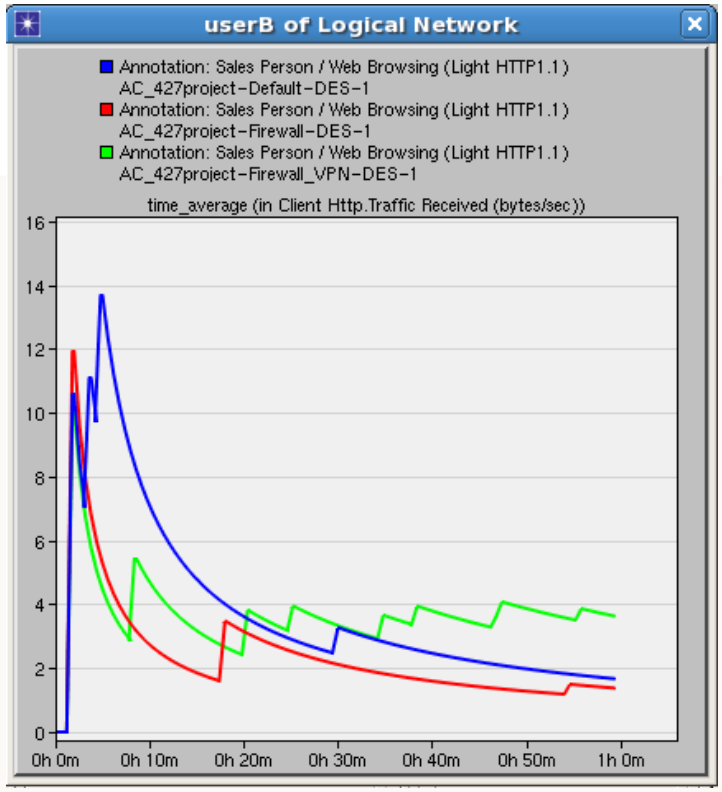
- UserA and UserB Database traffic received.
- UserA receives traffic in the default scenario and also in the VPN scenario since it was tunnelled to VPN_router.

Results and Discussion

Comparing userA and userB for HTTP traffic received



userA: HTTP Traffic Received



userB: HTTP Traffic Received

SFU

Results and Discussion

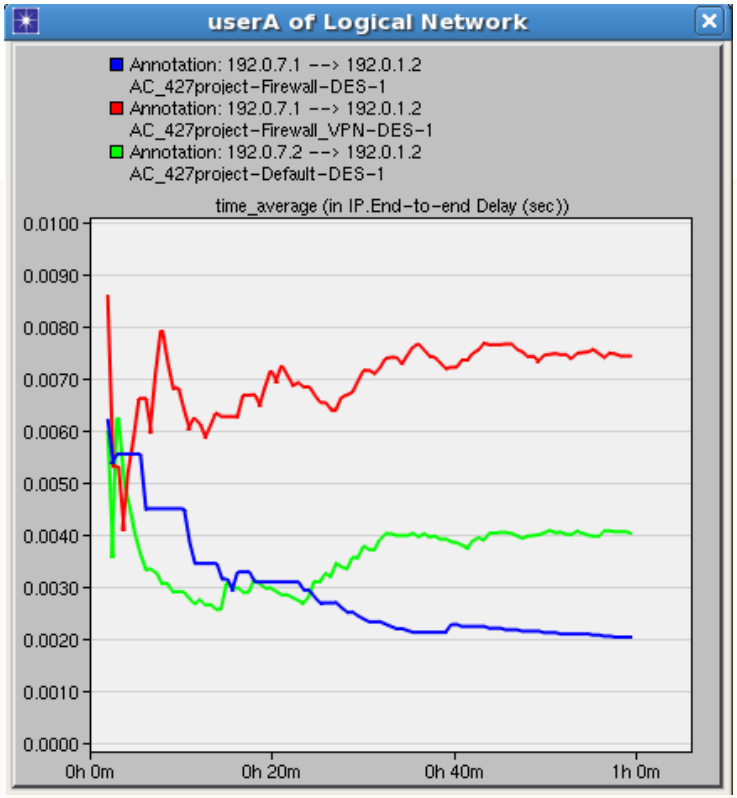
Comparison of traffic statistics between userA and userB

- Web browsing (HTTP) traffic received for User A and UserB

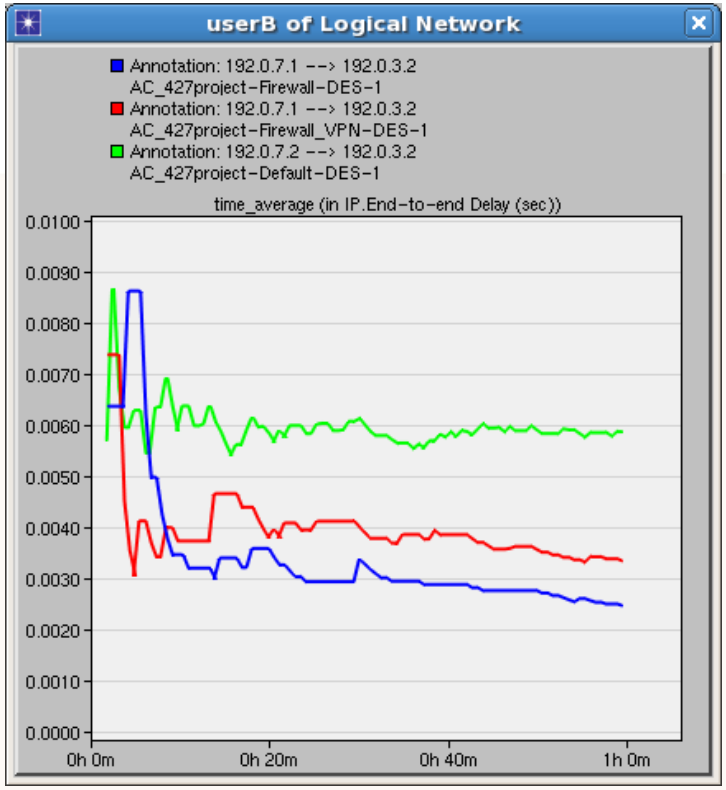
- Since no restriction was placed upon web browsing applications for all scenarios, it is expected that the received traffic at users A, B, and C remain fairly static

Results and Discussion

Comparing end-to-end packet delay



userA: end to end packet delay



userB: end to end packet delay

SFU

Results and Discussion

Comparing end-to-end packet delay

- End-to-end delay is the time it takes for a packet to travel across the network from the source to destination
- UserA saw more delay in the VPN configuration as opposed to the default and firewall scenarios
- In a VPN connection, the client and server are sending packets at the UPLOAD speed. Upload speed is usually much slower than download, hence the higher end-to-end delay
- UserB sees more delay in the default scenario mostly because no applications are blocked
- A higher traffic leading to longer delays will be expected.

Roadmap

- Motivation
- Background Information
- OPNET Simulation
- Results & Discussion
- Related Works
- Future Works
- Conclusion
- References

Related Works

- "Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN)". ICEIE 2010. Sapna, Sharma.
  - Compares the performance of firewalls and VPNs in a wired and wireless scenario
  - Examines which scenario is more secure for specific applications when both use a firewall and VPN
- "Performance Evaluation of a wired Network with & without Load Balancer and Firewall". 2010 International Conference on Recent Trends in Information, Telecommunications and Computing. Kosta, Dalal, Jha.
  - Examines performance of a WAN by comparing the effect of using a Load Balancer in a firewall
  - Tests the network against a variety of applications including FTP, ATM, remote login and Print

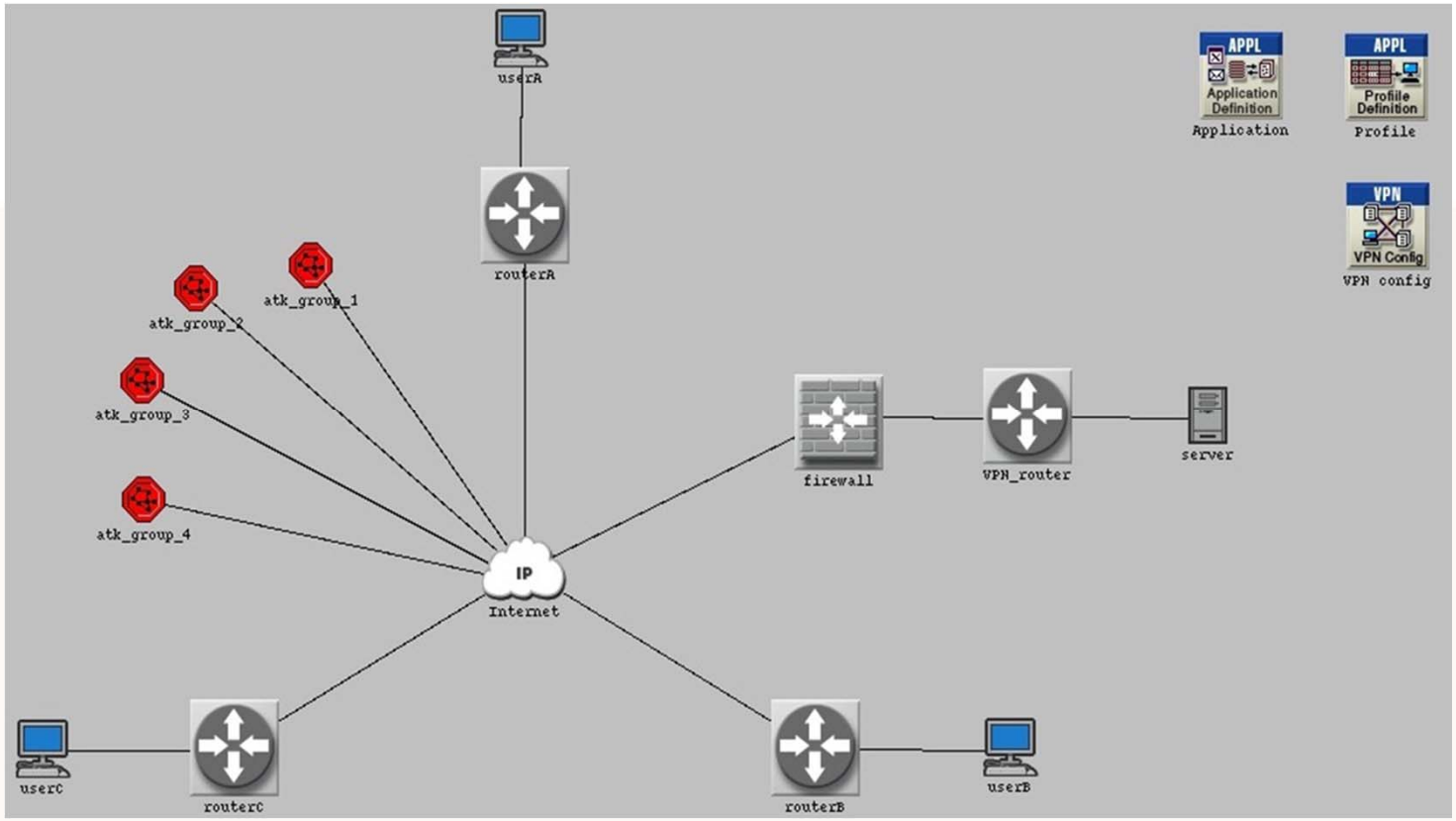
Roadmap

- Motivation
- Background Information
- OPNET Simulation
- Results & Discussion
- Related Works
- Future Works
- Conclusion
- References

Future Work

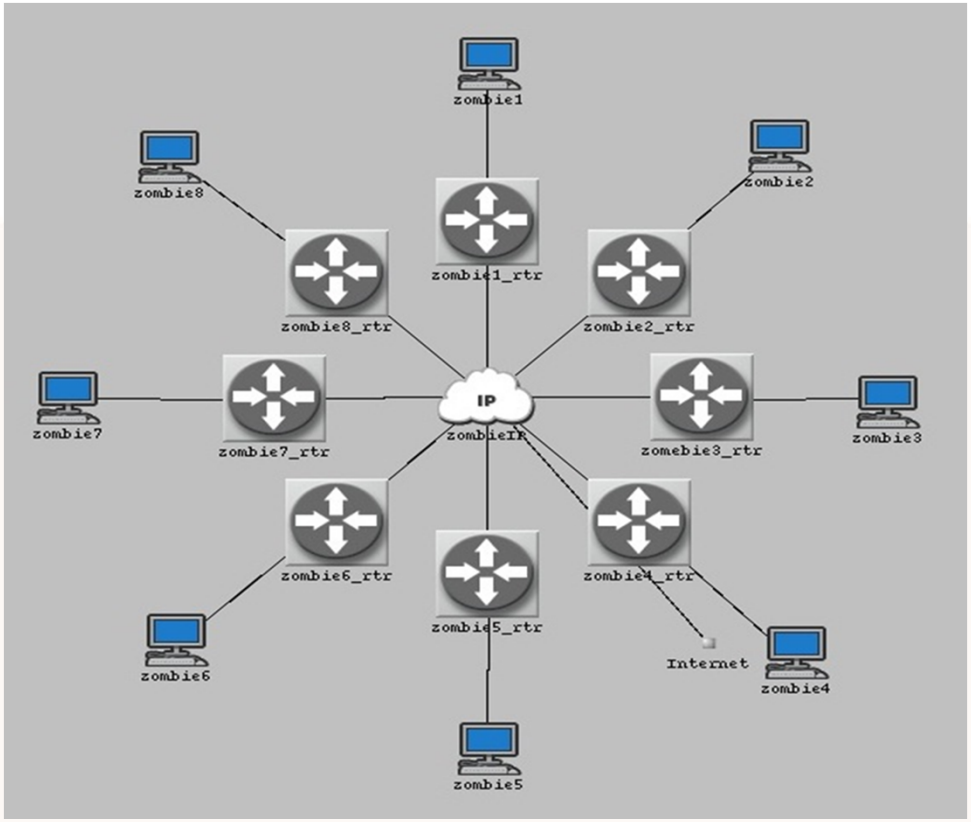
- The capabilities of a firewall can be fully understood when put under high traffic
- Such traffic includes illegitimate traffic such as Distributed Denial of Service attacks
- As a future improvement, we want to implement the topology below
- Each attacker subnet consists of 8 zombies, configured to simultaneously bombard the firewall with high traffic
- We can employ several different Quality of Service (QoS) congestion methods such as Priority Queuing (PQ) and Weighted Fair Queuing (WFQ)

Future Work



Topology of our existing VPN network with Attacker subnets

Future Work



Topology of Attacker subnet

SFU

Roadmap

- Motivation
- Background Information
- OPNET Simulation
- Results & Discussion
- Related Works
- Future Works
- Conclusion
- References

Conclusion

- Three different scenarios (default, firewall, VPN) were created and compared various statistics.
- To verify that firewalls preventing Database access properly, received traffic statistics were examined.
- Firewalls and VPNs introduce latency as observed, however it is mostly negligible.
- VPNs in general have more latency compared to firewalls, although this is also because the VPN router was placed behind the firewall
  - Traffic must pass through firewall first (more delay)
  - VPN traffic travels through each same LAN wire twice, degrading performance
  - Ex. From client to first VPN router, then VPN router encrypts data and then sends through the IP cloud to firewall

Roadmap

- Motivation
- Background Information
- OPNET Simulation
- Results & Discussion
- Related Works
- Future Works
- Conclusion
- References

References

[1] Y.P. Kosta, U.D Dalal, R.K Jha, “Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN)” in *2010 Int. Conf. on Recent Trends in Information, Telecommunications and Computing*. 2010.

[2] Sapna, M. Sharma, “Performance Evaluation of a wired Network with and without Load Balancer and Firewall”, in *2010 Int. Conf. on Electronics and Information Engineering, ICEIE 2010*. 2010.

[3] Ray Blair, Arvind Durai. (2009, May 21). *Chapter 1: Types of Firewalls* [Online]. Available: http://www.networkworld.com/subnets/cisco/060109-ch1-cisco-secure-firewalls.html?page=2

[4] Microsoft. *VPNs and Firewalls* [Online]. Available: http://technet.microsoft.com/en-us/library/cc958037.aspx

[5] Tech-faq. *Tunneling* [Online]. Available: http://www.tech-faq.com/tunneling.html

References

[6] Shabana Razak, Miam Zhou, S.H. Lang, “Network Intrusion Simulation using OPNET,” IEEE Computer Design and Applications Repository.

[7] Mian Zhou, “Network Intrusion Detection: Monitoring, Simulation and Visualization,” unpublished, 2005.

[8] K. Salah, A. Alkhoraidly. “An OPNET-based Simulation Approach for Deploying VoIP,” unpublished.

Thank You !

Questions?