|  |  |
| --- | --- |
|  | 3413ICT Network Security  School of Information & Communication Technology  Semester 1, 2014 |

**Assignment 2**

**(Weighting 10%)**

**Assignment Due: 23 May, Friday, 16:00 Hrs**

***Analysis of Effect of Secure Operations on the Performance of Medium-Scaled Wide Area Network Using OPNET***

***Student Name:*** *Anthony Guevara* ***E-mail:*** [***anthony.guevara@griffithuni.edu.au***](mailto:anthony.guevara@griffithuni.edu.au)

***Student #:*** *2877416*

1. **Problem Description**

In the assignment 1, we designed a technical security plan for the medium-scaled Wide Area Network owned by a Motel Chain. The CEO of the Motel Chain wants thorough analysis of the effect of e*ncryption* and c*ompression* operations on the performance of the network.

You are required to build a simulator, generate results and prepare a report describing analysis and your recommendations to the CEO.

1. **Requirements for the Simulator**
2. The two servers, namely, database and web servers are located at the Brisbane headquarters.
3. The Gold Coast LAN has two segments, namely, *official* (1 router and 5 workstations) and *client* (1 router and 10 mobile devices).
4. The *official* segment in the Gold Coast LAN can access all data including web services and database access.
5. The *client* segment, however, only has access to the web services.
6. The communication between *official* segment in the Gold Coast office and the *management* segment of the headquarters LAN should be compressed and encrypted.
7. The communication between *client* segment in the Gold Coast office and the *management* segment of the headquarters LAN should be compressed.
8. The simulator should include the following scenarios for comparison purpose:
   * Scenario 1: No firewall, VPN, encryption, and compression is employed, that is, a network without any protection.
   * Scenario 2: Only firewall is implemented between two branches.
   * Scenario 3: Employing firewall(s), VPN(s), encryption, and compression operations to meet the requirements (a) – (f) given above.
9. **Deliverables**

**Demonstration:** On Tuesday, 3rd June 2014 (Week 13) each student will be required to present findings of his/her work in 3 minute’s presentation and there will be a one minute Q&A session after each presentation.

**Report:** Each student must submit, a report comprising of following components.

Contents

[a) A summary of the addressed topic and the objectives of the project. 2](#_Toc388613937)

[b) Procedure of implementing the simulator, including the steps of creating and configuring the scenarios. 3](#_Toc388613938)

[c) Results obtained throughout the simulation. 9](#_Toc388613939)

[d) Analysis of the simulation results, a comparison of the results between scenarios, and a comparison of the simulation results with the theoretical expectations. 12](#_Toc388613940)

[e) How does the implementation of security techniques affect the network performance? 13](#_Toc388613941)

[f) A conclusion that includes your recommendations to the CEO of the Motel Chain. 14](#_Toc388613942)

# A summary of the addressed topic and the objectives of the project.

A client is looking to secure their network given three possible scenarios:

-VPN  
-firewalls  
-Both firewalls and VPN

The CEO of a motel chain has requested analysis be done on these three scenarios to see how compression and encryption affects network performance. These scenarios have been created using software called OPNET IT GURU to simulate the different scenarios and gain data on the different implementations. The following diagrams depict each scenario created in OPNET.

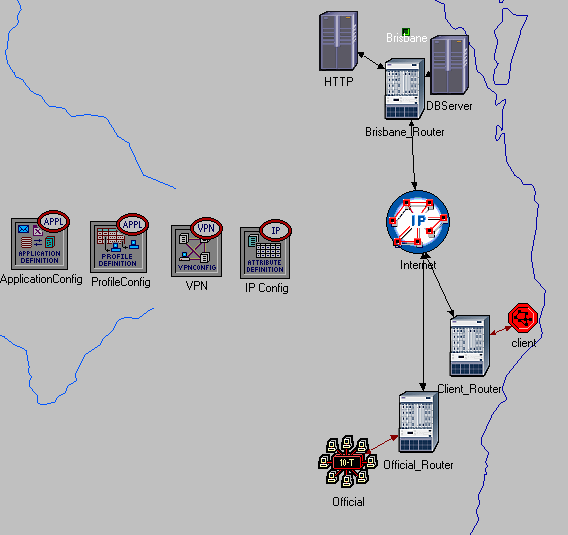


Figure 1.1 - VPN with compression and encryption on the Official LAN, compression on the client wireless LAN

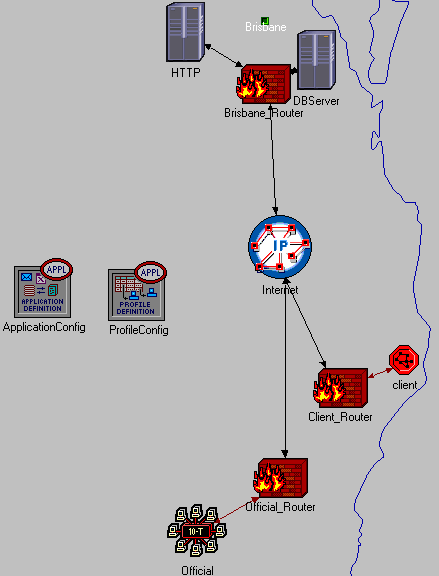


Figure 1.2 – No compression or encryption, only firewalls

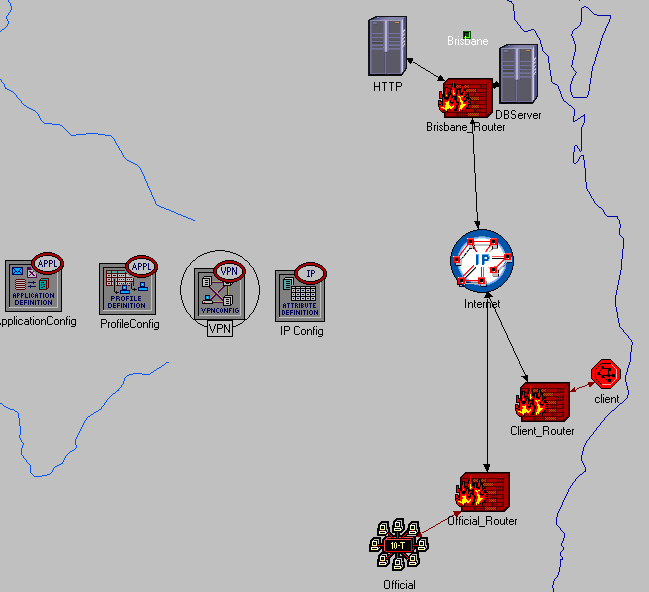


Figure 1.3 – VPN implemented on Official and client segments, in addition to implementing firewalls

# Procedure of implementing the simulator, including the steps of creating and configuring the scenarios.

1. Create a new scenario
2. Assign the project name Assignment2

Assign the Scenario Name: Assignment2\_VPN

1. Select Create Empty Scenario

-Choose From Maps

-**Australia**

-Next

-**OK**

1. Open Object Palette and drop the following objects onto the scenario:

|  |  |  |  |
| --- | --- | --- | --- |
| Object Name | Palette | Number | Configuration(right click, edit attributes) |
| Application Config | Internet\_toolbox | 1 | Name: ApplicationConfig  Application Definition->rows: set to 4  Application Definition Row 0 config:    Application Definition Row 1 config:    Application Definition Row 2 config:    Application Definition Row 3 config:  -N/A only used for testing |
| Profile Config | Internet\_toolbox | 1 | Name: ProfileConfig    Profile Configuration->rows: set to 4  Profile Configuration Row 0 config:    Profile Configuration Row 1 config:    Profile Configuration Row 2 config:    Profile Configuration Row 3 config:  -N/A only used for testing |
| IP VPN Config | Internet\_toolbox | 1 | Name: VPN |
| IP Attribute Config | Internet\_toolbox | 1 | Name: IP Config  IP Compression Information->row 3(Default Per-Virtual Circuit Compression) config: |
| Ethernet4\_slip8\_gtwy | Internet\_toolbox | 3 | Gateway1: -Name: Brisbane\_Router  Gateway2:  -Name: Client\_Router Gateway3:  -Name: Official\_Router |
| Ppp\_server | Internet\_toolbox | 2 | Name: HTTP  Http Server:    Db Server:  Name: DBServer |
| 10BaseT\_LAN | Internet\_toolbox | 1 | Name: Official  Set up compression on the LAN:  IP Host Parameter->Interface Information->Compression Information: |
| Ip32\_cloud | Internet\_toolbox | 1 | Name: Internet |
| subnet | Internet\_toolbox | 1 | Name: Client  All of the wlan\_wkstn go in the Client subnet |
| Wlan\_ethernet\_router | Wireless\_lan | 1 | Name: Access Point |
| Wlan\_wkstn | Wireless\_lan | 10 | Name: Wkstn\_x where x is numbers 1 to 10  Set up compression for each workstation:  IP Host Parameters->Interface Information->Compression Information: |

Objects should be set up to look like Figure 1.1 in section a). The following table lists the appropriate connections between interfaces:

|  |  |  |
| --- | --- | --- |
| Point A | Point B | Connection Link |
| Official | Official\_Router | 10BaseT |
| Access Point | Client\_Router | 10BaseT |
| HTTPServer | Brisbane\_Router | PPP\_DS1 |
| DBServer | Brisbane\_Router | PPP\_DS1 |
| Official\_Router | Internet | PPP\_DS1 |
| Client\_Router | Internet | PPP\_DS1 |

**Firwall Scenario**:

Scenario->Duplicate Scenario

Name the new scenario: Assignment2\_Firewall

1. Replace all the routers with firewalls. Right click on a router->Select Similar Nodes  
2. Right click on a router->Edit Attributes->Tick box in left corner (Apply Changes to Selected Objects)  
3. Change object to firewall: Model->(Change to ethernet2\_slip8\_firewall)  
4. Delete VPN and IP Config since they will not be used in the firewall scenario  
5. Ensure the scenario looks like Figure 1.2 in section a)

**Firewall and VPN Scenario:**

Switch back to scenario 1 “Assignment2\_VPN”  
Scenario->Duplicate Scenario  
Name the new scenario: Assignment2 \_VPN\_Firewall

1. Replace all the routers with firewalls. Right click on a router->Select Similar Nodes  
2. Right click on a router->Edit Attributes->Tick box in left corner (Apply Changes to Selected Objects)  
3. Change object to firewall: Model->(Change to ethernet2\_slip8\_firewall)  
4. Ensure the scenario looks like figure 1.3 in section a)

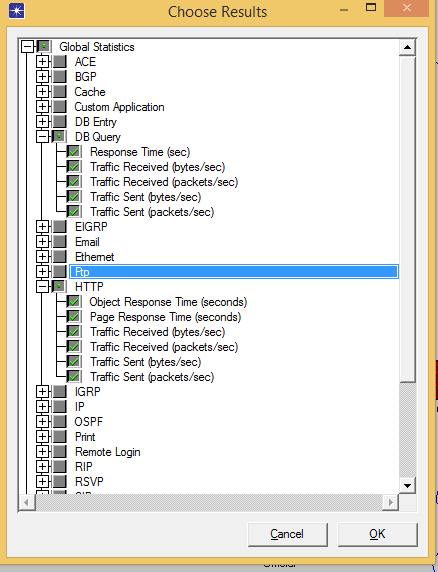
**Statistics collected:**

Right click on scenario->Choose Individual Statistics

->Global Statistics->

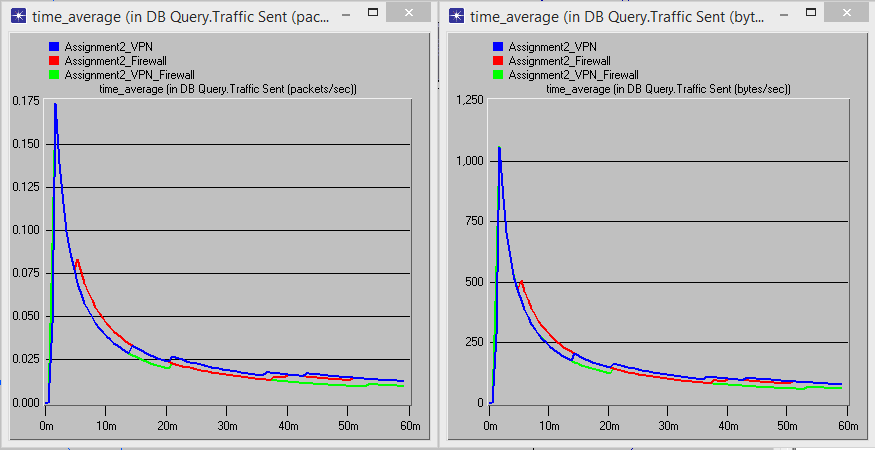
->Select DB Query

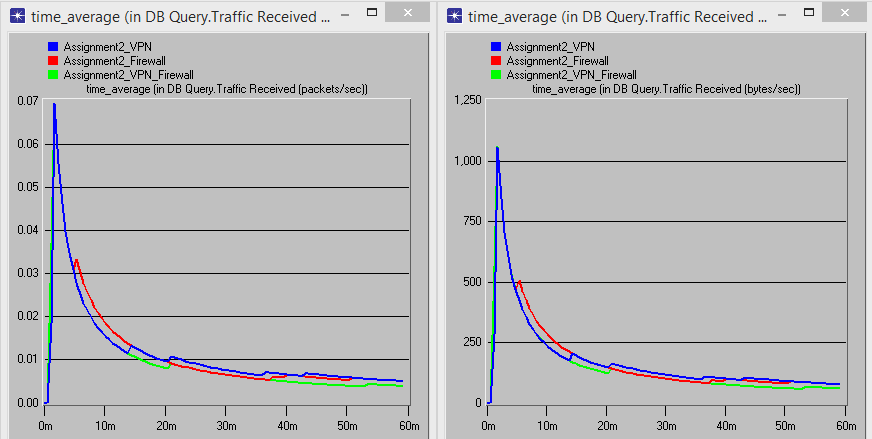
->Select HTTP

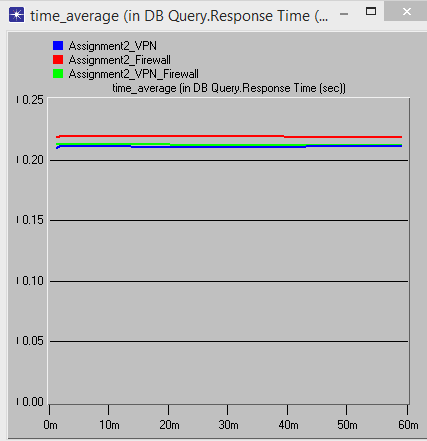


# Results obtained throughout the simulation.

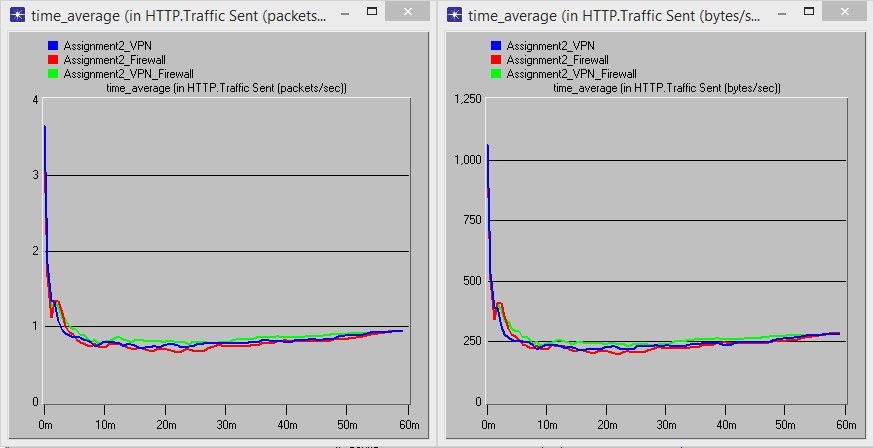
DBQuery Simulation Results:

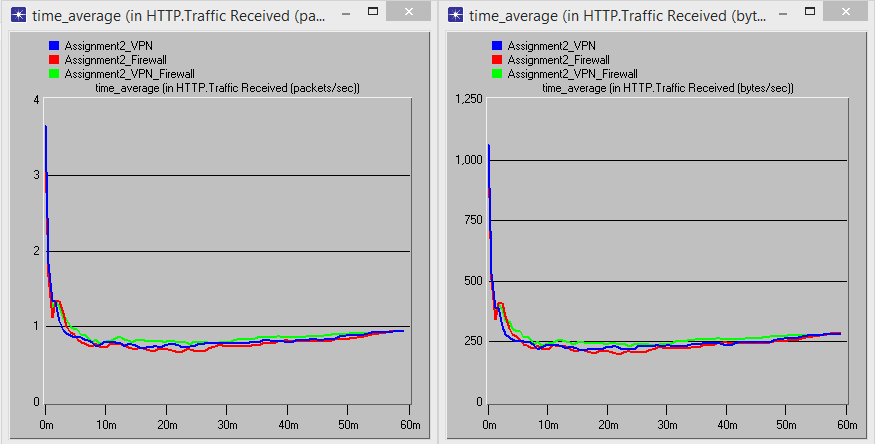


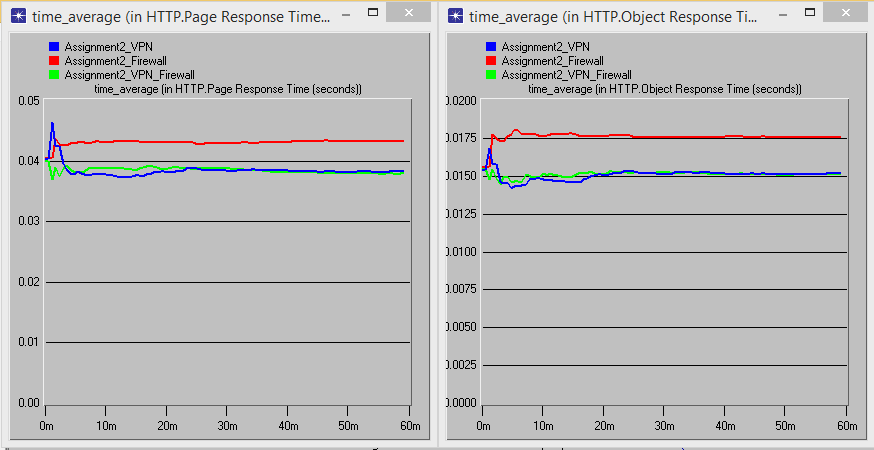




HTTP Results:







# Analysis of the simulation results, a comparison of the results between scenarios, and a comparison of the simulation results with the theoretical expectations.

The data collected from the simulation includes DBQuery traffic and HTTP traffic. The data was collected using a 1 hour simulation interval in a network with no background traffic. This section will begin by looking at the results of the DBQuery traffic and then move to analysing HTTP traffic results.

The DBQuery results follow very similar trends for all three scenarios relating to traffic sent (packets/sec and bytes/sec). There is an abnormal spike in the charts that occurs in the firewall only scenario. This may be caused due the firewall dealing with additional processing time included in the proxy servers because it operates at a higher OSI layer level.

Traffic received (packets/sec and bytes/sec) was also slightly higher for the firewall at the ten minute mark, this could also be related to the firewall proxy behaving as an application level retransmission device and not implementing compression. The response time was highest for the firewall only scenario. The VPN and firewall combined had slightly better response times due to implementing compression. VPN had the quickest DBQuery response time of the three scenarios because it was using compression without the overhead of using a firewall.

HTTP traffic sent was highest in the combined VPN and firewall scenario. Adding additional security mechanisms also adds additional computing cycles and time. Additionally, the data received was directly proportional to the data sent. Therefore, the VPN and firewall scenario put out the most traffic and received the most traffic. VPN placed second, and the firewall scenario had least amount of traffic sent/received.

Page response time and object response time were the highest in the firewall scenario for HTTP traffic. Again, the assumption behind the poor performance is related to the firewalls proxy deployed services. VPN performed second best, and combined firewall and VPN performed the best.

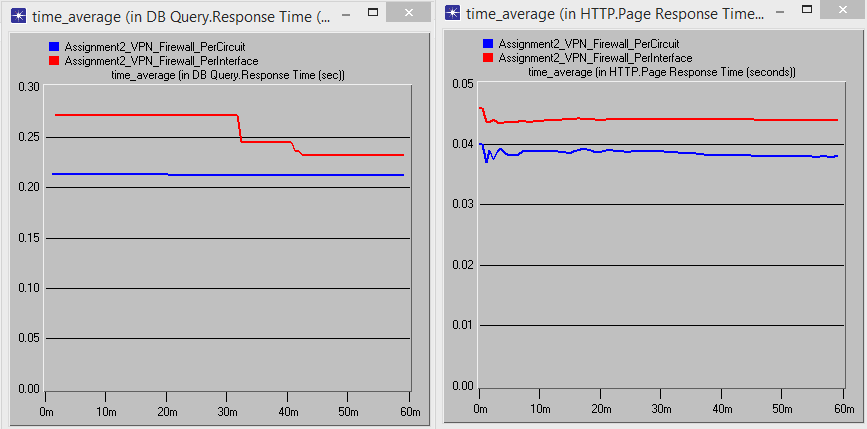
Overall, the firewall only scenario performed the worst of the three different scenarios. The reason for poor performance was due to the firewall not being used in a busy network with background traffic. The firewall scenario truly shines where it can block unnecessary traffic and permit legitimate traffic. Had there been a higher volume of different types of traffic, especially more data intensive traffic such as video and voice, a firewall would be more efficient and the results would be more in there favour.

# How does the implementation of security techniques affect the network performance?

Network performance suffers as the number of security parameters increases. For example, encryption and decryption add additional overhead and processing time. One of the limitations of using the OPNET simulator is that different encryption algorithms were not taken into consideration when using encryption over VPN. This leaves the user to guess an approximate encryption delay time measured in seconds.

Compression is another parameter which adds additional overhead, especially if configured incorrectly. Compression is added to the Official LAN segment as well as the client LAN segment using the ‘Per-Virtual Circuit Compression’ method.

The ‘Per-Virtual Circuit Compression’ method operates by compressing data only at the starting and ending nodes, which cuts down on computation delays. Compared to ‘Per-Interface Compression’ which is more computationally expensive, compression and decompression take place at every hop. The following diagram demonstrates the difference between the two:



From these results above we can infer that per circuit (blue) operates quicker than per interface (red) for database query response time and http response time.

A simulator is great tool for testing out different networking parameters because a diverse set of options can be configured and deployed virtually without real hardware. Once the network has been tested thorough simulation, the results can be analysed and decisions can be made based on the results. A simulator has a number of practical applications: such as being used to show clients a working theoretical implementation of a network, and being able to collect and compare different network statistics. The main benefit of the simulator is being able to discover how changing certain parameters affect other parts of the network.

It is important to select the most appropriate algorithms to satisfy security services. Selecting the incorrect implementation could be quite costly and negatively impact network performance. It is equally crucial to have an understanding of how certain configurations work. For example, understanding how the different compression and encryption algorithms affect the operation of a network. Using the simulator provides a test environment to discover and work out these issues. The results from the various scenarios have provided data stating that as more security services are added, the less efficient the network performs in the absence of background traffic.

# A conclusion that includes your recommendations to the CEO of the Motel Chain.

Based on the results of each scenario I would recommend implementing a VPN only scenario. Nearly all of the data results were very close to each other making all three implementations viable options. VPN is recommended because it is the cheapest options to implement because the least amount of hardware is required. Many routers today support point to point tunnelling and are implemented in software. Taking into consideration how small the network is (only 5 workstations on official, 10 on client), a VPN network would be adequate for the gold coast Official and client LAN.

A hotel typically wouldn’t be interested in upgrading the infrastructure of the Official segment. The customer and client side of the network would receive more monetary funding to ensure the clients remain happy with the wireless internet service. While a VPN implementation will be fine for the Official segment, it is not recommended for the client segment. If the motel plans on expanding the client segment, and the number of theoretical wireless clients jump from 10 to 100, the network performance may suffer.

As the number of clients continues to grow, the network will undoubtedly develop additional background traffic. Clients will most likely be streaming data such as music and video which will consume large amounts of network bandwidth. It is estimated that 1/2 of all data traffic on the internet is video from YouTube and Netflix. Having a firewall in this case would be extremely useful to limit or block the amount of data that can be accessed from web video streaming.

The best implementation for the CEO would be to implement a VPN for the Official segment of the LAN and use a firewall for the client segment. The VPN will provide compression and encryption services that take place over a point to point tunnel satisfying the Official LAN requirements. A firewall will allow access control rules to be setup, which allow blocking or throttling particular types of traffic such as video. This will allow excellent service to be maintained by filtering unnecessary traffic that could potentially diminish the quality of service offered by the client segment.  
  
In conclusion, data has been collected from three simulations to see which performs the quickest. Attached in the subfolder OPNET is a project that includes the three different simulations (Assignment2\_VPN, Assignment2\_Firewall, and Assignment2\_VPN\_Firewall). Section B provides steps for setting up the simulation, in addition to showing the different configurations used for each object. Section C provides graphical results of DBQuery and HTTP traffic collected for the different scenarios. Section D discussed the collected results and how they compared to what was expected. Section E discussed the pros and cons of adding security mechanisms and how it affects network performance. It has been found through analysis of data that the client segment should implement a firewall, and the Official LAN should implement a VPN.