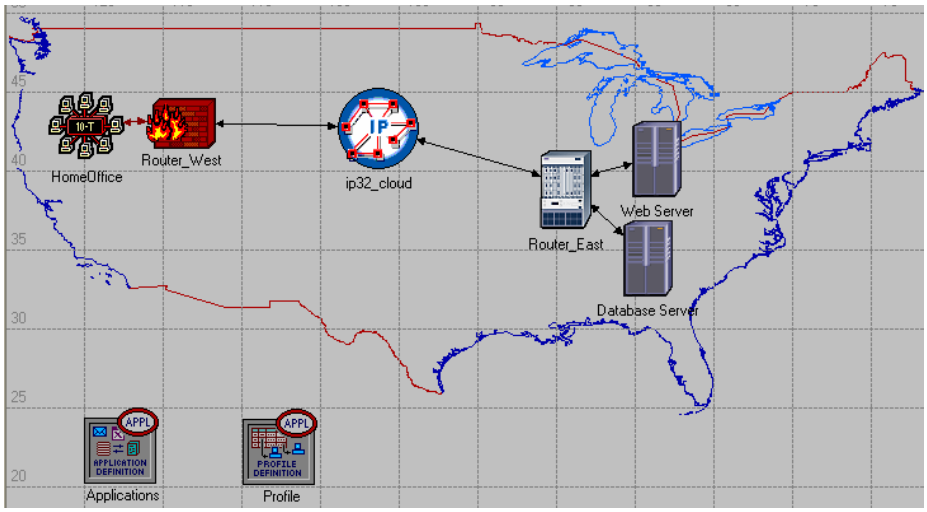
CSE 4482: Security Lab 1

Firewall Performance

This lab has been partially based on "OPNET Lab Manual To Accompany Data and Computer Communications", by Kevin Brown and Leann Christianson, Prentice Hall, 2004.



Objective

The goal of this lab is examine the effect of firewall filtering on application response time.

Overview

A firewall is a router which provides additional security functionality. Firewalls are commonly deployed at the border of a corporate network and the Internet, and are used to monitor and regulate the traffic that passes through this border. Firewalls inspect various header fields in packets as they arrive and, based on a security policy, choose to discard (filter) the packets, or forward them on to the destination. Packets may be filtered based on the source or destination IP address, the source or destination port number, or other header fields. For instance, a corporate site's firewall could be configured to accept only packets originating at the corporation's other locations, or only packets destined for the FTP port. All other packets would be discarded to protect the corporation's devices from unwanted access. While firewalls provide a valuable service, the additional filtering functionality can require extra processing time, possibly lowering throughput.

Lab Instructions

IT Guru consists of **projects** and **scenarios**. A project comprises one or more network scenarios. Each scenario represents a different **what-if** analysis performed by the users. Scenarios may contain different versions of the same network or models of different networks.

In this lab, we will build and analyze the performance of a corporate network consisting of two segments: the home-office (i.e. client system) in the West and the server system in the East. The two segments are connected through the Internet, which makes them (potentially) vulnerable to malicious/unwanted traffic.

The lab requires you to create 3 different scenarios in order to compare the performance of the same (topological) network in the following three cases: 1) there is no firewall in the network, 2) there is a firewall in the network and it allows all traffic through, 3) there is a firewall in the network and it discards web traffic.

Step 1: Build the Simulation Model

1. Start IT Guru.

2. Select **File** → **New …** choose **Project** and click **OK**.

3. Set the **Project Name** to **xx_Firewall** (where **xx** are your initials). Set the **Scenario Name** to **No_Firewall**. Click **OK**.

4. In the **Initial Topology** window, select **Create Empty Scenario** and click on **Next**.

5. In the **Choose Network Scale** window, select **World** and click on **Next**.

6. In the **Choose Map** window, choose **usa** and click on **Next**.

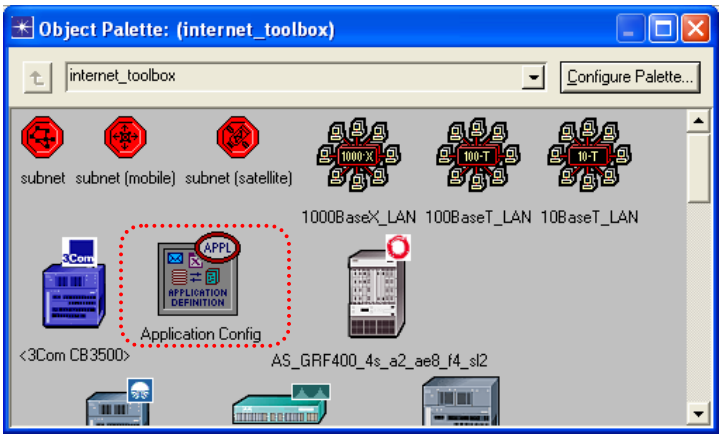
7. In the **Select Technologies** window, click on **Next**.

8. In the **Review** window, click **OK**.

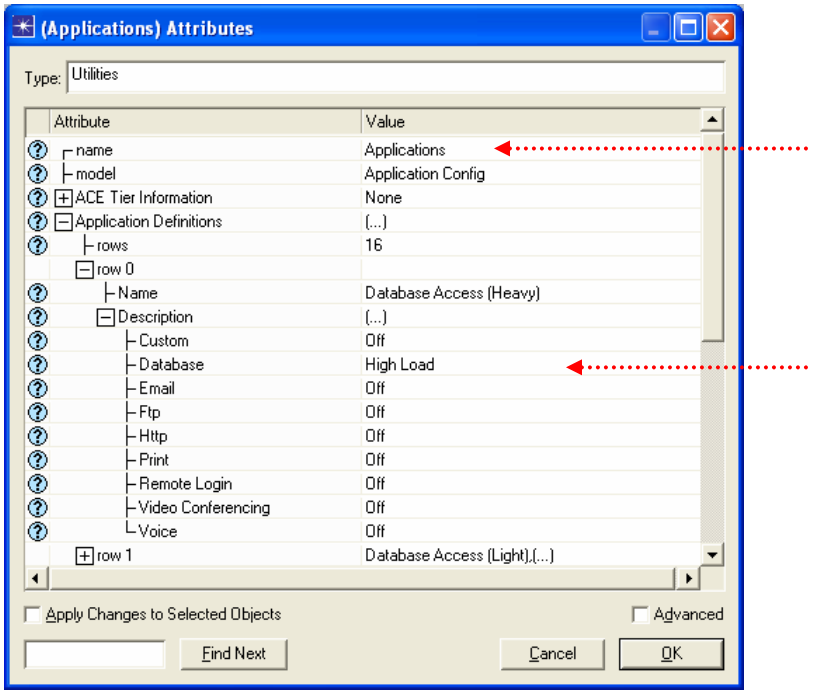
Next, we will configure the traffic profiles for our users. We need one profile for the motivated workers, who will perform database transactions, and one profile for the idle workers, who will do web browsing.

Step 1.a: Build Traffic Profiles for Applications and Users

1. Select an **Application Config** object from the Object Palette  and place it in the project workspace.



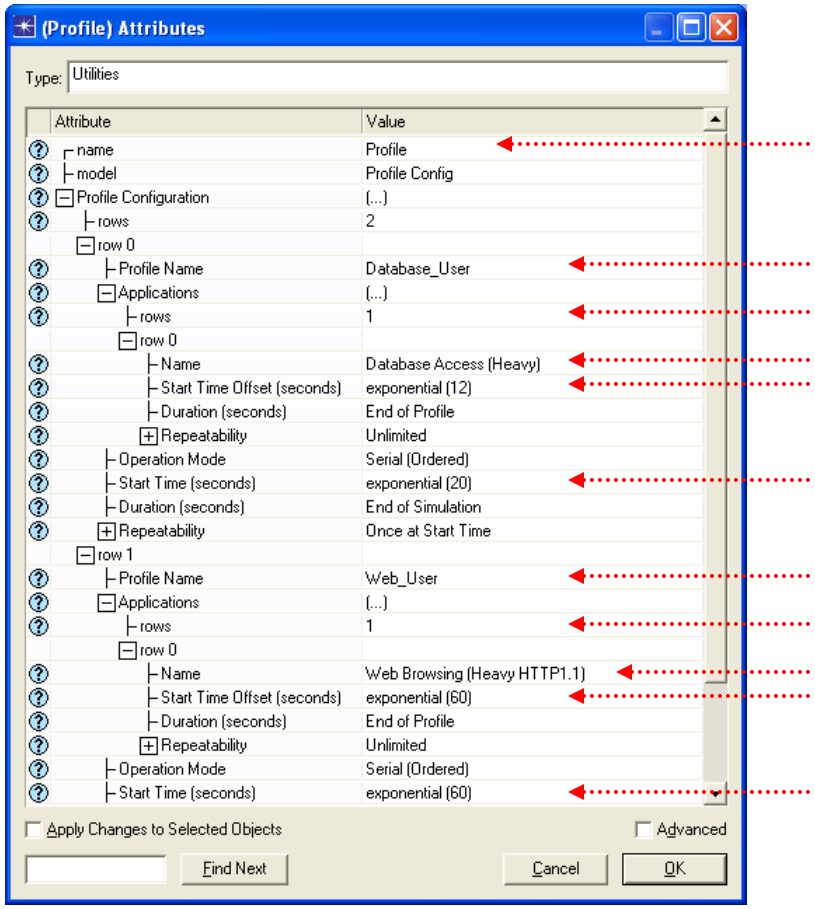
2. Right click on the object and choose **Edit Attributes**. Set Applications Attributes as follows:
   a) Set the **name** to **Applications**.
   b) Set the **Application Definitions** attribute to **Default**. We can now use or modify the default applications defined by OPNET, including web browsing, FTP, and others.
   c) Expand the **Application Definitions** attribute and the **row 0** attribute (which describes the **Database Access (Heavy)** application).
   d) Expand the **Description** attribute and modify the **Database** attribute to **High Load**.
   e) Click on **OK** to close the window.



3. Select a **Profile Config** object 

from the Object Palette and place it in the project workspace.

4. Right click on the object and choose **Edit Attributes**. Set Profile Attributes as follows:



a) Set the **name** to **Profiles**.
b) Expand the **Profile Configuration** attribute and set the **rows** attribute to **2**.
c) Expand the **row 0** attribute, and set the **Profile Name** to **Database_User**.
d) Expand the **Applications** attribute, and set the **rows** attribute to **1**.
e) Expand the **row 0** attribute, and set the **Name** to **Database Access (Heavy)**.
f) Set the **Start Time Offset (seconds)** to **exponential(12)**.
g) Set the **Start Time (seconds)** for the profile (which is the second Start Time attribute) to **exponential(20)**.
h) Expand the **row 1** attribute, and set the **Profile Name** to **Web_User**.
i) Expand the **Applications** attribute , and set the **rows** attribute to **1**.
j) Expand the **row 0** attribute, and set the **Name** to **Web Browsing (Heavy HTTP1.1)**.
k) Set the **Start Time Offset (seconds)** to **exponential(60)**.
l) Set the **Start Time (seconds)** for the profile (which is the second Start Time attribute) to **exponential(60)**.

(*Note: The start time values will cause the large number of users (100) to be spread over a long interval so that they do not all start at once.*)

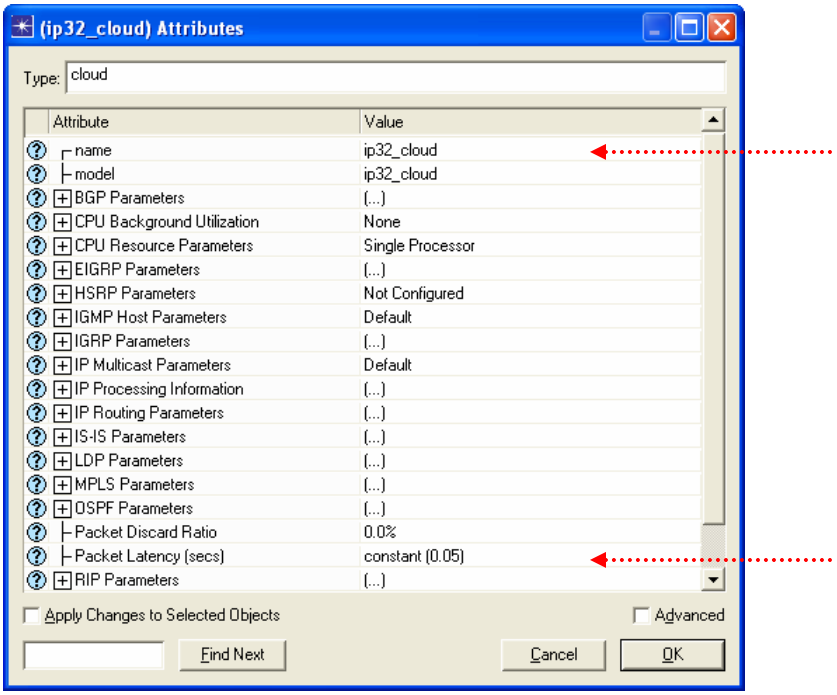
m) Click on **OK** to close the window.

Step 1.b: Create Client System in the West

1. Select an **ip32_cloud** object  from the Object Palette and place it in the project workspace.

2. Right click on the cloud and choose **View Node Description**. The cloud represents a WAN consisting of IP-capable routers that supports up to 32 serial links.

3. Right click on the cloud and select **Edit Attributes**.
   a) Set the name to **ip32_cloud**.
   b) Set the **Packet Latency (secs)** to **constant(0.05)**. You will need to change the **Special Value** to **Not Used** in order to modify the Packet Latency value. This implies that any packet which passes through the cloud will now experience a delay of 50 milliseconds.
   c) Click on **OK** to close the window.



4. Select an **ethernet4_slip8_gtwy** device  from the Object Palette and place it in the project workspace.

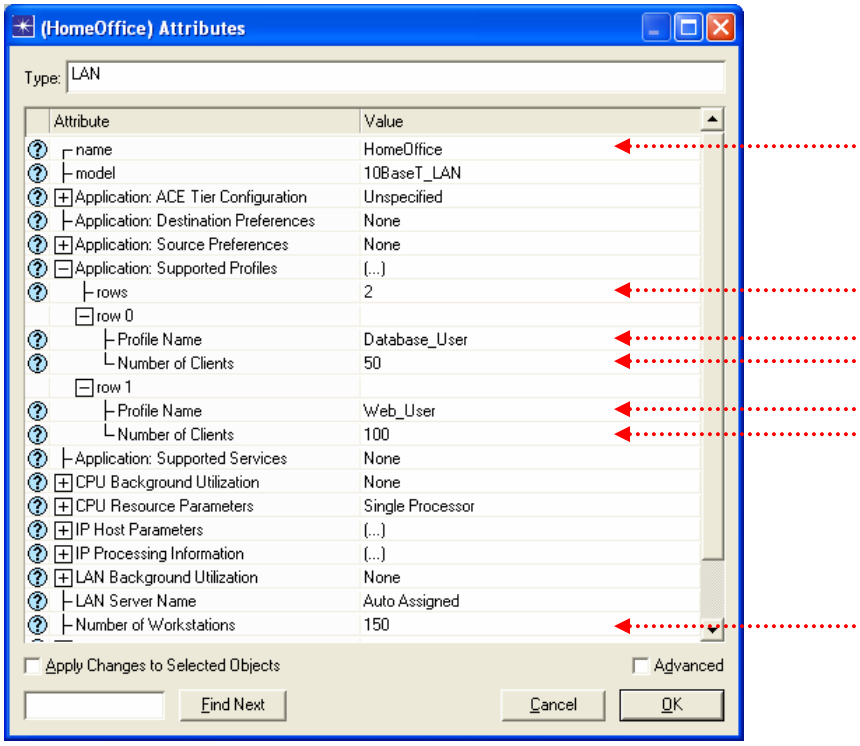
5. Right click on the station and choose **View Node Description**. Note that the station supports both the Ethernet and SLIP protocols.

6. Right click on the station and choose **Set Name**. Set the **Name** to **Router_West**. Click on **OK** to close the window.

7. Select a **10BaseT_LAN** object  from the Object Palette and place it in the project workspace.

8. Right click on the LAN and choose **View Node Description**. Note that the LAN object represents multiple workstations and supports various applications. Click on the close window icon to close the window.

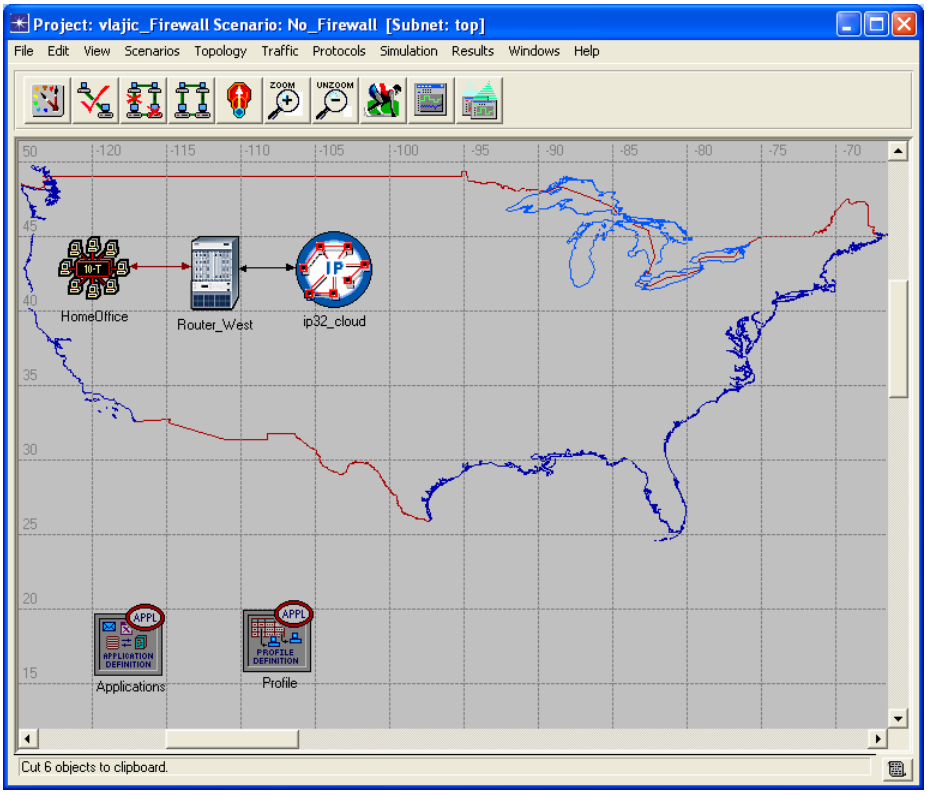
9. Right click on the LAN and choose **Edit Attributes**.
   a) Modify the **name** attribute of the LAN to **Home Office**.
   b) Set the **Number of Workstations** to **150**.
   c) Expand the **Application: Supported Profiles** attribute, and set the **rows** attribute to **2**.
   d) Expand the **row 0** attribute, and set the **Profile Name** to **Database_User**. Set the **Number of Clients** to **50**.
   e) Expand the **row 1** attribute, and set the **Profile Name** to **Web_User**. Set the **Number of Clients** to **100**.
   f) Click on **OK** to close the window.



10. Select a **10BaseT** link  from the Object Palette and use it to connect the Home Office to **Router_West**.

11. Select a **PPP_DS1** link  from the Object Palette and use it to connect the **Router_West** to the ip32_cloud.

12. Remember that DS1 speed is 1.5 Mbps.



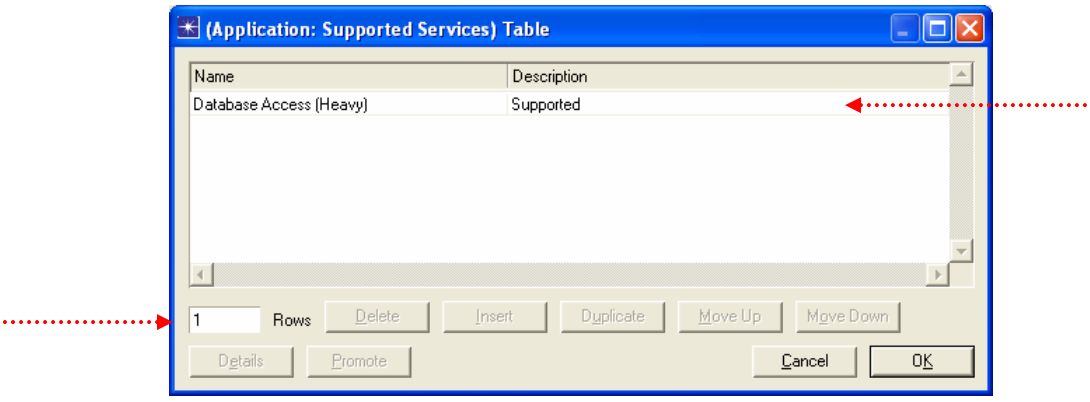
Step 1.c: Create Server System in the East

1. Select an **ethernet4_slip8_gtwy** device  from the Object Palette and place it in the project workspace.

2. Right click on the station and choose **Set Name**. Set the **Name** to **Router_East**. Click on **OK** to close the window.

3. Select a **ppp_server** device  from the Object Palette and place two copies in the project workspace.

4. Right click on the first server and choose **Edit Attributes**.
   a) Set the **name** to **Database Server**.
   b) Edit the **Application: Supported Services** attribute, and set the number of **rows** to **1**.
   c) Edit the **Name** field of the first row and set to **Database Access (Heavy)**.
   d) Click on **OK** twice to close the windows.



5. Right click on the second server and choose **Edit Attributes**.
   a) Set the **name** to **Web Server**.
   b) Edit the **Application: Supported Services** attribute, and set the number of **rows** to **1**.
   c) Edit the **Name** field of the first row and set to **Web Browsing (Heavy HTTP1.1)**.
   d) Click on **OK** twice to close the windows.

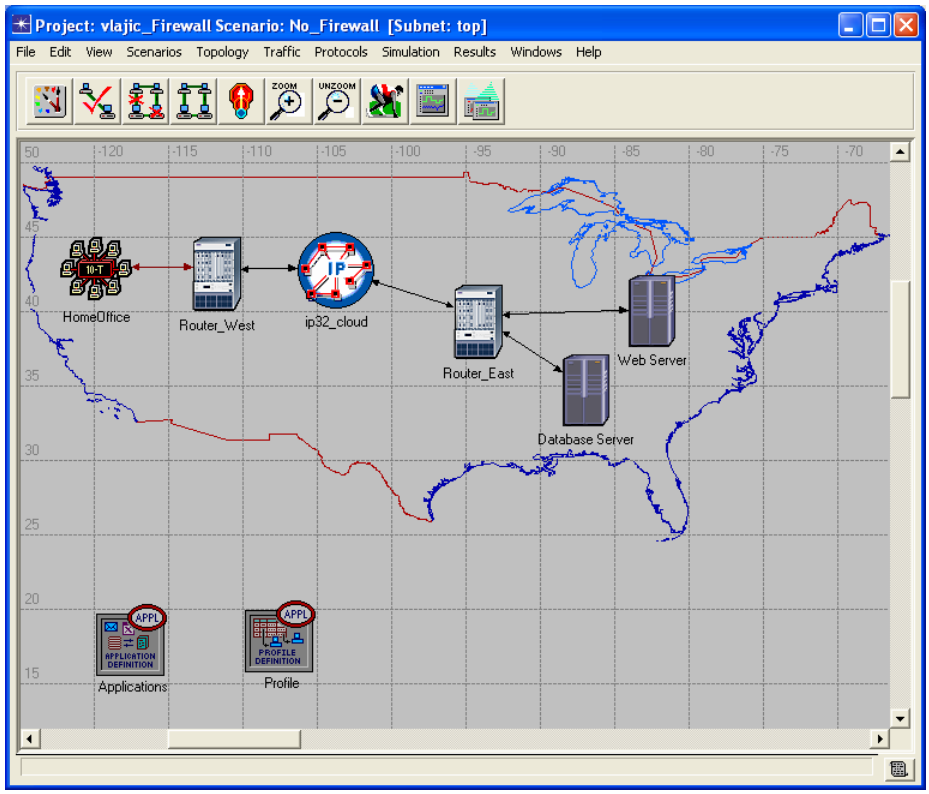
7. Select two **PPP_DS3** links 

from the Object Palette and use them to connect the Database Server to **Router_East**, and the Web Server to **Router_East**.

8. Select a **PPP_DS1** link 

and use it to connect **Router_East** to the ip32_cloud.

Your network setup should now look as follows:



Step 2: Configure the Simulation

1. Select the **Simulation** tab => **Choose Individual Statistics…**

2. Expand the **Global Statistics** item and the **DB Query** item, and select the **Response Time (sec)** statistic.

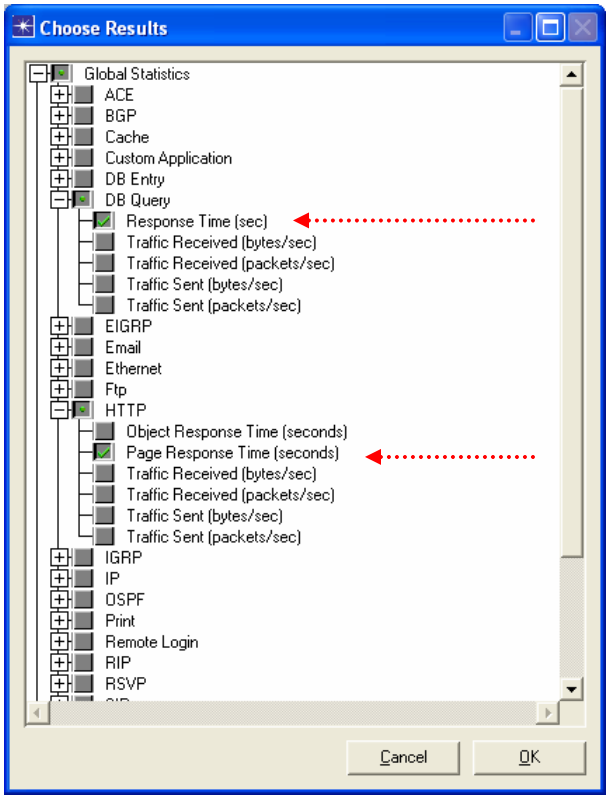
3. Expand the **HTTP** item and select the **Page Response Time (seconds)** statistic.

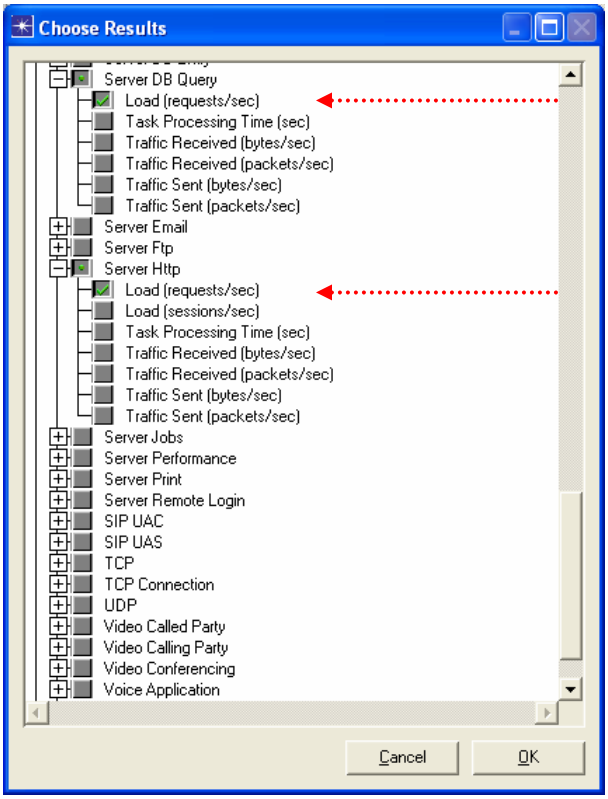
4. Expand the **Node Statistics** item and the **Server DB Query** item, and select the **Load (requests/sec)**.

5. Expand the **Server HTTP** item and select the **Load (requests/sec).**

6. Expand the **Link Statistics** and the **point-to-point** item, and select the **utilization <--** and **utilization -->** statistics.

7. Click on **OK** to close window.

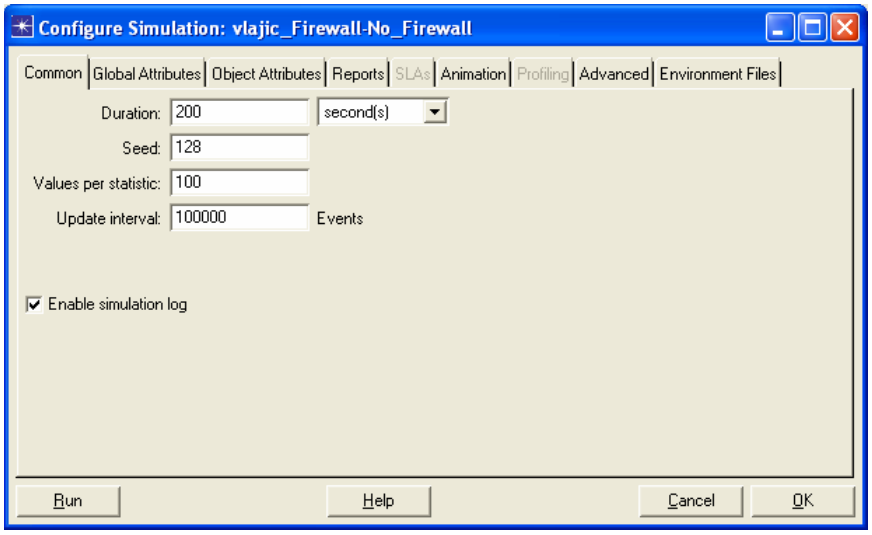




8. Select **Simulation => Configure Discrete Event Simulation…**

9. Under the **Common** tab, set the **Duration** to **200**, and the unit to **second(s)**.

10. Click on **OK** to close the window.



Step 3: Duplicate the Scenario (Firewall)

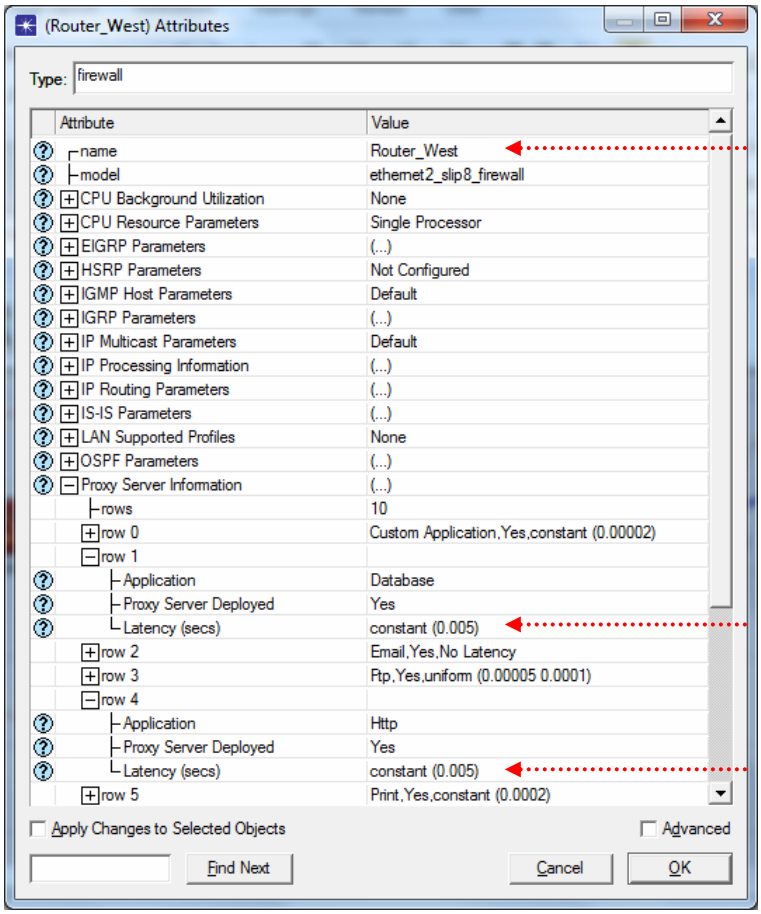
We are now going to duplicate the scenario to model a network with a firewall replacing **Router_West**. We will create one scenario in which the firewall allows traffic through, but adds processing delay due to the packet filtering required. We will create another scenario in which the firewall discards web traffic. This will allow us to compare the database performance application in these different instances.

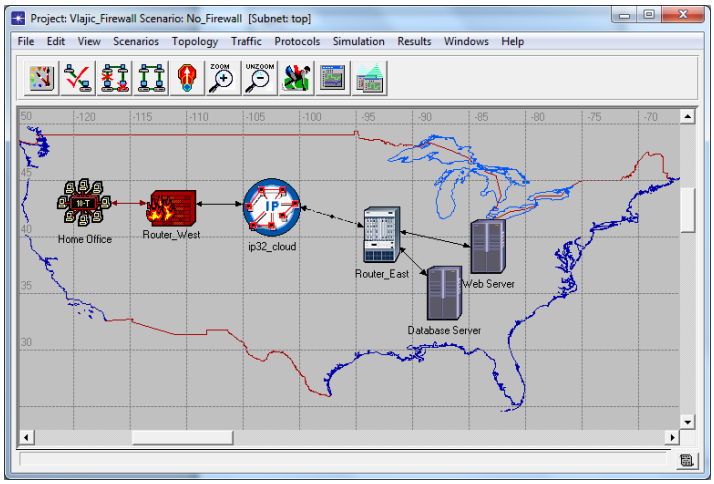
1. Choose **Scenarios** => **Duplicate Scenario**, and name the new scenario **Firewall**.

2. Right click on **Router_West**, and choose **Edit Attributes**.
   a) Edit the **model** and choose **ethernet2_slip8_firewall** from the pull-down menu.
   b) Expand the **Proxy Server Information** attribute and the **row 1** attribute (which describes the Database Proxy behavior). Set the **Latency** to **constant(0.005)**.
   c) Expand the **row 4** attribute (which describes the HTTP Proxy behavior) and set the **Latency** to **constant(0.005)**.

      *Note that both applications show **Proxy Server Deployed** set to **yes**. This means that the firewall will allow traffic generated by these two applications to pass through.*

   d) Click on **OK** to close the window and replace the gateway with the firewall.





Step 4: Duplicate the Scenario (Firewall_Blocking)

1. Choose **Scenarios** => **Duplicate Scenario** again, and name the new scenario **Firewall_Blocking**.

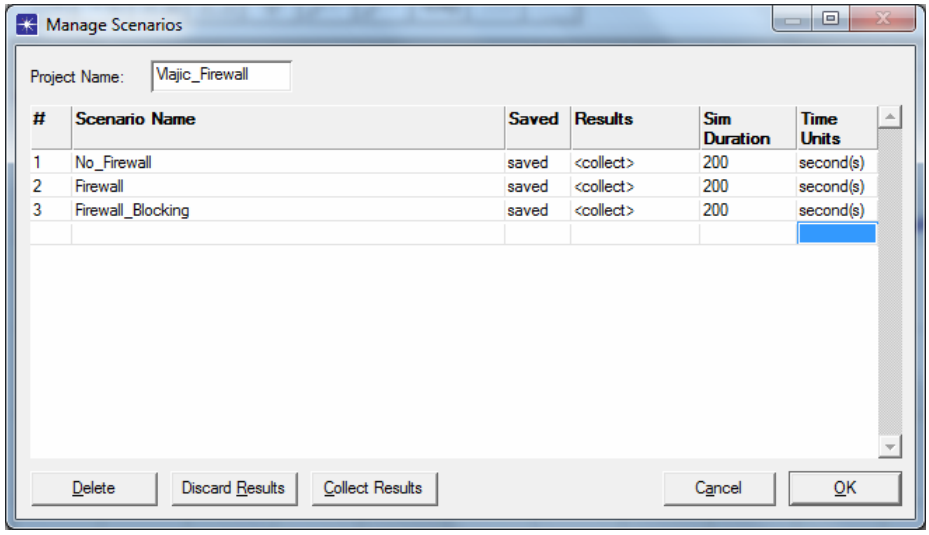
2. Right click on **Router_West**, and choose **Edit Attributes**.
   a) Expand the **Proxy Server Information** attribute, and the **row 4** attribute (which describes the HTTP Proxy behavior).
   b) Set the **Proxy Server Deployed** attribute to **no**. This means that the firewall will discard all web traffic.
   c) Click on **OK** to close the window.

Step 5: Run the Simulation

1. Select the **Scenarios** tab => **Manage Scenarios…**

2. Edit the **Results** field for all three rows and set the value to **<collect>** or **<recollect>**.

3. Click on **OK** to run the scenarios (one after the other).



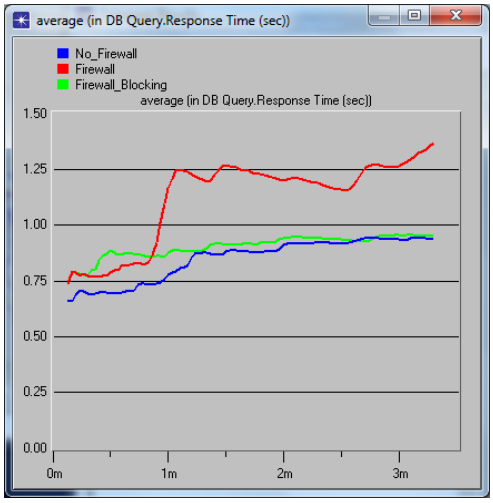
When the simulation has completed, click on **Close** to close the window.

Step 6: Inspect and Analyze Results

1. Select the **Scenarios** tab => **Switch to Scenario.** Switch to the **No_Firewall** scenario.

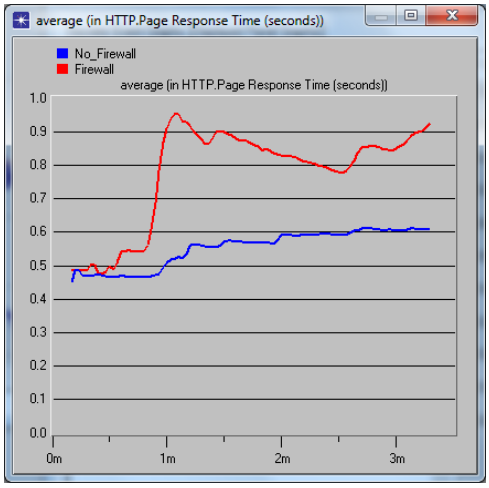
2. Select the **Results** tab => **Compare Results…**

3. Expand the **Global Statistics** item and the **DB Query** item, and select the **Response Time (sec)** statistic. This statistic shows how long each database query took to complete. Use **average** mode to view the statistic. Click on **Show** to see a more detailed graph. Your graph should resemble the graph shown below.



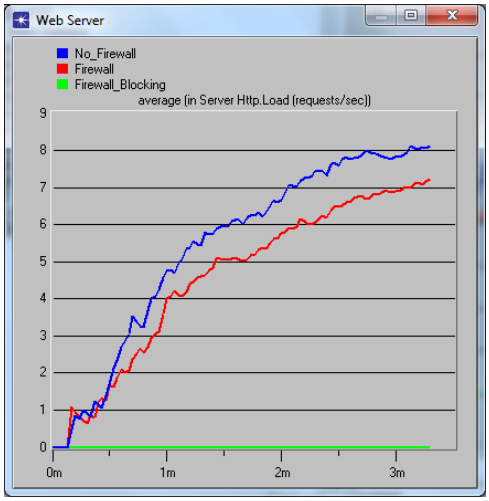
QUESTION 1
Your task is to take a screenshot of your own graph obtained by performing Step 6.3, and include it in the final report. You are also required to comment on the obtained results, i.e. explain the cause of the difference among the three plots and their respective values?

4. Expand the **HTTP** item and select the **Page Response Time (seconds)** statistic. View the statistic using **average** mode. Click on **Show** to see a more detailed graph. Your graph should resemble the graph shown below.



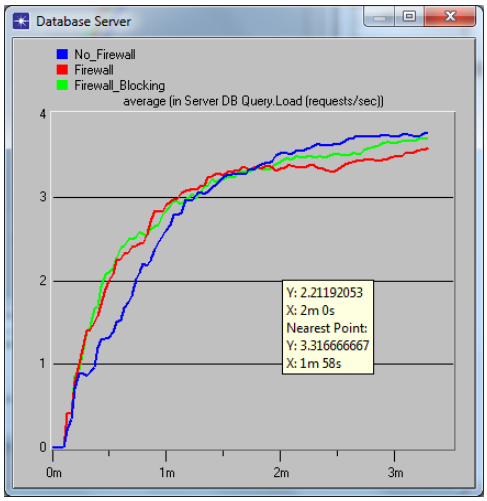
QUESTION 2
Again, your task is to take a screenshot of your own graph obtained by performing Step 6.4, and include it in the final report. Once again, explain the cause of the difference among the obtained plots and their respective values?

5. Expand the **Object Statistics** item, the **Web Server** item, and the **Server HTTP** item. Select the **Load (requests/sec)** statistic and use **average** mode to view the statistic. Click on **Show** to see a more detailed graph. Your graph should resemble the graph shown below.



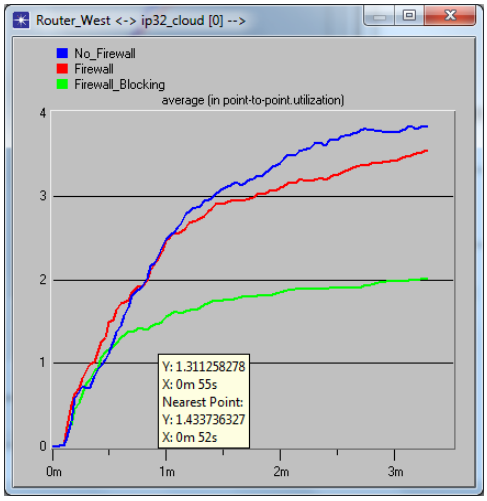
QUESTION 3
Include the screenshot of your own graph obtaineld by performing Step 6.5 in the final report. How do you explain the difference among the obtained plots and their respective values?

6. Expand the **Object Statistics** item, the **Database Server** item, and the **Server DB Query** item. Select the **Load (requests/sec)** statistic and use **average** mode to view the statistic. Click on **Show** to see a more detailed graph. Your graph should resemble the graph shown below.



QUESTION 4
Include the screenshot of your own graph obtaineld by performing Step 6.6 in the final report. How do you explain the difference between the graph obtained in this question (Database Server Load), and the one from Question 3 (Web Server Load)?

7. Expand the **Router_West <-> ip32_cloud[0]** item, and the **point-to-point** item, and select the **utilization ->** statistic. (This statistic shows the amount of traffic that was seen on the DS1 link between **Router_West** and the WAN.) Use **average** mode to view the statistic. Click on **Show** to see a more detailed graph. Your graph should resemble the graph shown below.



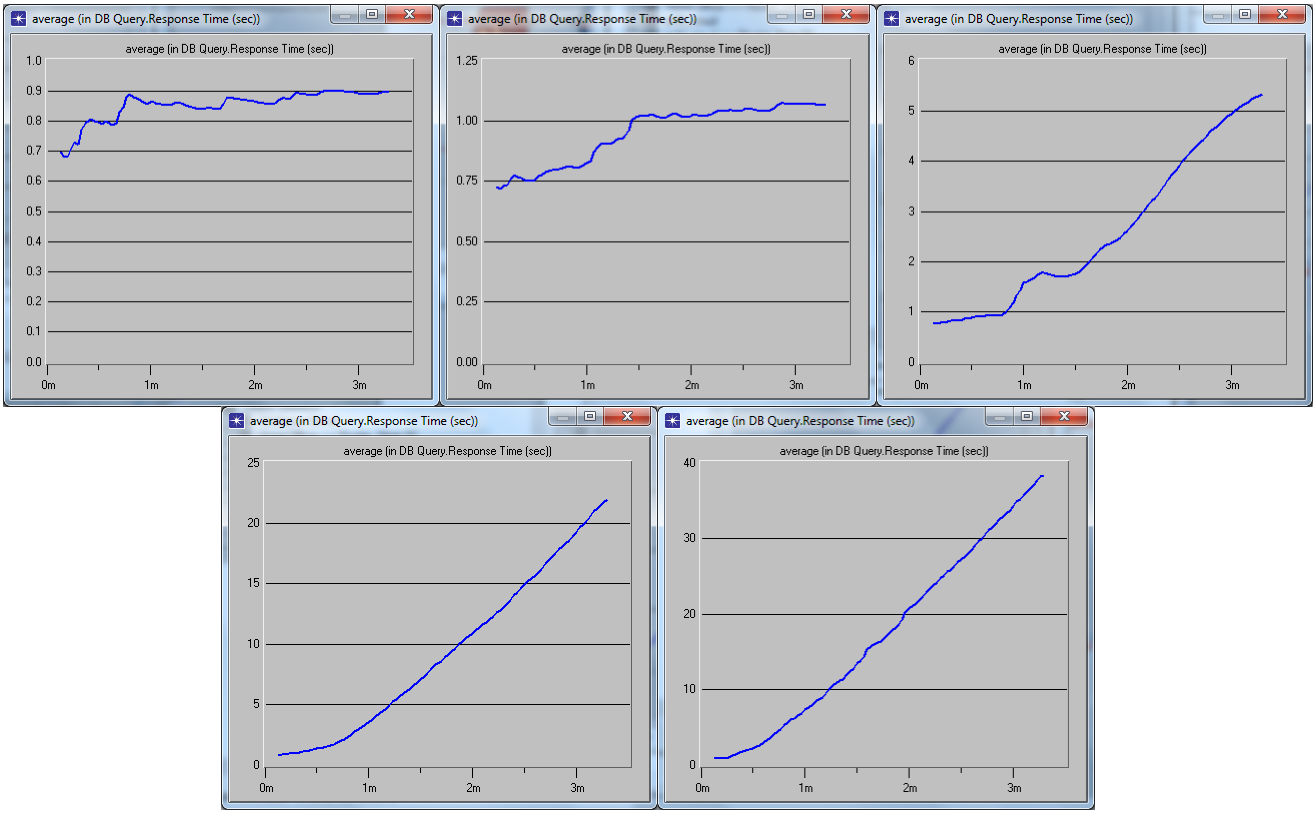
QUESTION 5

Include the screenshot of your own graph obtaineld by performing Step 6.7 in the final report. How do you explain the difference among the obtained plots and their respective values?

QUESTION 6

Firewalls can often act as bottlenecks if they are unable to forward packets at the same rate that they receive them. Duplicate the Firewall scenario and name it **Firewall_Latency**. Edit the Proxy attributes of the firewall, and set the latency for the Database application to constant(0). Rerun the simulation and record the DB Query Response Time. Repeat for values of 0.004, 0.006, 0.008, and 0.01. Graph your values and explain your results.

Answer to Q6


average (in DB Query.Response Time (sec))
average (in DB Query.Response Time (sec))
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
0m
1m
2m
3m
average (in DB Query.Response Time (sec))
average (in DB Query.Response Time (sec))
1.25
1.00
0.75
0.50
0.25
0.00
0m
1m
2m
3m
average (in DB Query.Response Time (sec))
average (in DB Query.Response Time (sec))
6
5
4
3
2
1
0
0m
1m
2m
3m
average (in DB Query.Response Time (sec))
average (in DB Query.Response Time (sec))
25
20
15
10
5
0
0m
1m
2m
3m
average (in DB Query.Response Time (sec))
average (in DB Query.Response Time (sec))
40
30
20
10
0
0m
1m
2m
3m