Laboratory
11

Firewalls and VPN

Network Security and Virtual Private Network

Objective

The objective of this lab is to study the role of the firewalls and virtual private networks in providing security to shared-public network such as the Internet.

Overview

Computer networks are typically a shared resource used by many applications for many different purposes. Sometimes the data transmitted between application processes is confidential, and the applications would prefer that others not be able to read it.

A firewall is a specially programmed router that sits between a site and the rest of the network. It is a router in the sense that it is connected to two or more physical networks and it forwards packets from one network to another, but it also filters the packets that flow through it. A firewall allows the system administrator to implement a security policy in one centralized place. Filter-based firewalls are the simplest and most widely deployed type of firewall. They are configured with a table of addresses that characterize the packets they will, and will not, forward.

The *virtual private network* (VPN) is an example of providing a controlled connectivity over a public network such as the Internet. VPN utilizes a concept called *IP tunnel*. IP tunnel is a virtual point-to-point link between a pair of nodes that are actually separated by an arbitrary number of networks. The virtual link is created within the router at the entrance to the tunnel by providing it with the IP address of the router at the far end of the tunnel. Whenever the router at the entrance of the tunnel wants to send a packet over this virtual link, it encapsulates the packet inside an IP datagram. The destination address in the IP header is the address of the router at the far end of the tunnel, while the source address of that of the encapsulating router.

In this lab you will set up a network where servers are accessed over the Internet by customers who have different privileges. You will study how firewalls and VPNs can provide security to the information in the servers while maintaining access for customers with the appropriate privilege.

Procedure

Creating a new project

1. Start the **OPNET** modeler and from the **File** menu, choose **New**.

2. Select **Project** and click **OK**. Name the project **YourInitials_VPN**, and the scenario **NoFirewall**. Click **OK**.

3. Click **Quit** on the *Startup Wizard*.

4. To remove the world background map, select the **View** menu ⇒ **Background** ⇒ **Set Border Map** ⇒ Select **NONE** from the drop-down menu ⇒ Click **OK**.

Creating and Configuring the network

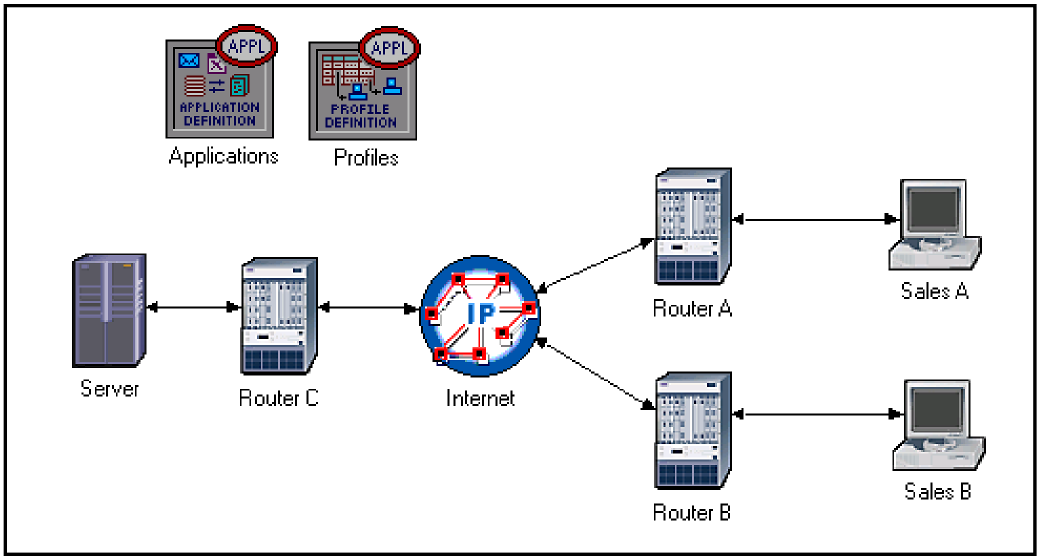
Network Initialization:

1. Open The *Object Palette* dialog box by clicking . Make sure that the opened palette is the one of the **internet_toolbox**.

2. Add to the project work space the following objects from the palette: **Application Config**, **Profile Config**, an **IP Clound**, one **ppp_server**, three **ethernet4_slip8_gtwy**, and two **ppp_wkstn**.

   a. To add an object from a palette, **Left-Click** its icon in the object palette ⇒ **Drag** it to the workspace ⇒ **Right-click** when finished placing the object.

3. Rename the objects you added and connect them using **PPP Ds1** cables as shown:



4. **Save** your project.

Configure the Nodes:

1. **Right** click on the **Applications** node ⇒ **Edit Attributes** ⇒ Assign **Default** to the **Application Definitions** attribute ⇒ Click **OK**.

2. **Right** click on the **Profiles** node ⇒ **Edit Attributes** ⇒ Assign **Sample Profiles** to the **Profile Configuration** attribute ⇒ Click **OK**.

3. **Right** click on the **Server** node ⇒ **Edit Attributes** ⇒ Assign **All** to the **Application: Supported Services** attribute ⇒ Click **OK**.

4. **Right** click on the **Sales A** node ⇒ **Select Similar Nodes** (make sure that both **Sales A** and **Sales B** are selected)

   i. **Right** click on the **Sales A** node ⇒ **Edit Attributes** ⇒ Check the **Apply Changes to Selected Objects** check box.

   ii. Add one **row** to the **Application: Supported Profiles** attribute ⇒ Expand **row 0** hierarchy ⇒ **Profile Name** = **Sales Person** (this is one of the “sample profiles” we configured in the *Profiles* node)

   iii. Click **OK**.

5. **Save** your project.

Choose Statistics

1. **Right-click** anywhere in the project workspace and select **Choose Individual Statistics** from the pop-up menu.
2. In the *Choose Results* dialog, check the following statistic :
   i. **Global Statistics** ⇒ **DB Query** ⇒ **Response Time (sec)**
   ii. **Global Statistics** ⇒ **HTTP** ⇒ **Page Response Time (sec)**

3. Click **OK**.

4. **Right-click** on the **Sales A** node and select **Choose Individual Statistics** from the pop-up menu.
5. In the *Choose Results* dialog, check the following statistic:
   i. **Node Statistics** ⇒ **Client DB** ⇒ **Traffic Received (bytes/sec)**
   ii. **Node Statistics** ⇒ **Client HTTP** ⇒ **Traffic Received (bytes/sec)**

6. Click **OK**.

7. **Right-click** on the **Sales B** node and select **Choose Individual Statistics** from the pop-up menu.

8. In the *Choose Results* dialog, check the following statistic:
   i. **Node Statistics ⇒ Client DB ⇒ Traffic Received (bytes/sec)**
   ii. **Node Statistics ⇒ Client HTTP ⇒ Traffic Received (bytes/sec)**

9. Click **OK** and **Save** your project.

The Firewall Scenario

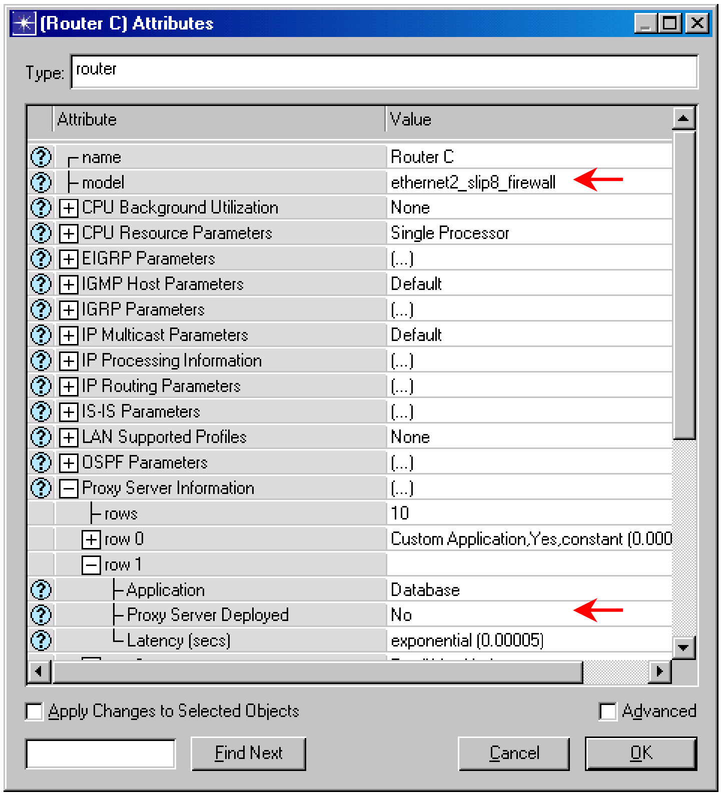
In the network we just created the *Sales Person* profile allows both sales sites to access applications such as *Database Access*, *Email*, and *Web Browsing* from the server (check the *Profile Configuration* of the *Profiles* node). Assume that we need to protect the database in the server from external access, including the sales persons. One way to do that is to replace *Router C* with a *Firewall* as follows:

1. Select **Duplicate Scenario** from the **Scenarios** menu and name it **Firewall**.

2. In the new scenario, right click on **Router C** ⇒ **Edit Attributes**.

3. Assign **ethernet2_slip8_firewall** to the **model** attribute.

4. Extend the hierarchy of the **Proxy Server Information** attribute ⇒ Extend **row 1**, which is for the *Database* application, hierarchy ⇒ Assign **No** to the **Proxy Server Deployed** attribute as shown:



Type: router

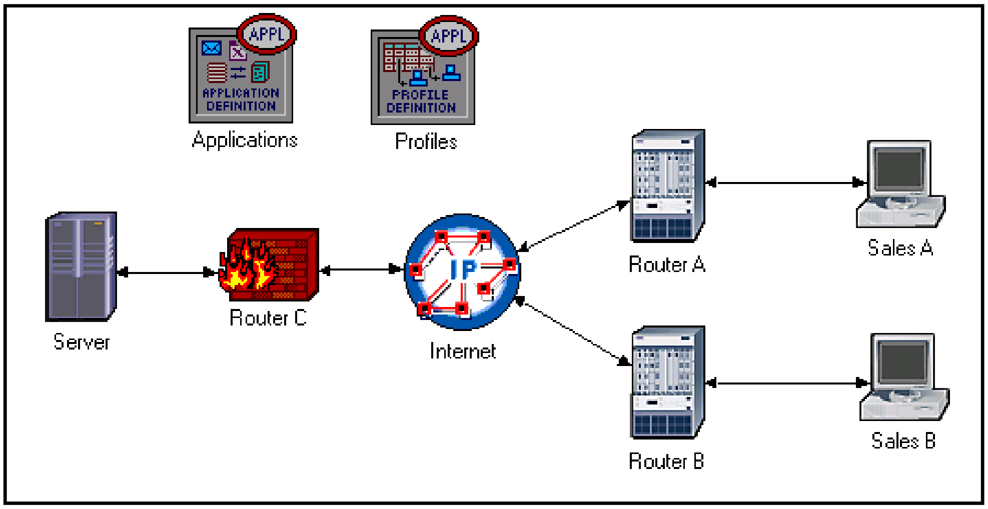
Attribute	Value
name	Router C
model	ethernet2_slip8_firewall
CPU Background Utilization	None
CPU Resource Parameters	Single Processor
EIGRP Parameters	(...)
IGMP Host Parameters	Default
IGRP Parameters	(...)
IP Multicast Parameters	Default
IP Processing Information	(...)
IP Routing Parameters	(...)
IS-IS Parameters	(...)
LAN Supported Profiles	None
OSPF Parameters	(...)
Proxy Server Information	(...)
rows	10
row 0	Custom Application,Yes,constant (0.000
row 1	
Application	Database
Proxy Server Deployed	No
Latency (secs)	exponential (0.00005)

□ Apply Changes to Selected Objects

□ Advanced

5. Click **OK** and **Save** your project.

Our *Firewall* configuration does not allow database-related traffic to pass through the firewall (it filters them out). This way the databases in the server is protected from external access. Your *Firewall* scenario should look like the following figure.



The Firewall_VPN Scenario

In the *Firewall* scenario, we protected the databases in the server from “any” external access using a firewall router. Assume that we want to allow the persons in the *Sales A* site to have access to the databases in the server. As the firewall filters all database-related traffic regardless of the source of the traffic, we need to consider the VPN solution. A virtual tunnel can be used by *Sales A* to send database requests to the server. The Firewall will not filter the traffic created by *Sales A* because the IP packets in the tunnel will be encapsulated inside an IP datagram.

1. While you are in the *Firewall* scenario, select **Duplicate Scenario** from the **Scenarios** menu and give it the name **Firewall_VPN**.

2. Open The *Object Palette* dialog box by clicking . Make sure that the opened palette is the one of the **internet_toolbox**.

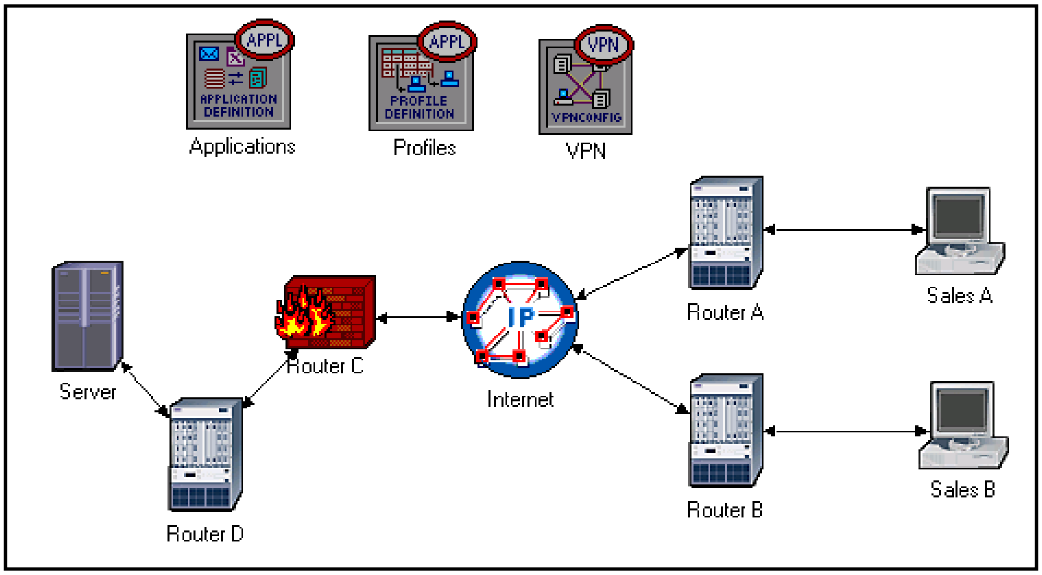
3. Add to the project workspace one **ethernet4_slip8_gtwy** and one **IP VPN Config.**

4. From the *Object Palette* use two **PPP Ds1** cables to connect the new router to the **Router C** (the firewall) and to the **Server**.

5. Remove the old link between Router C and Server.

6. Rename the **IP VPN Config** object to **VPN**.

7. Rename the new router to **Router D** and as shown:



Configure VPN:

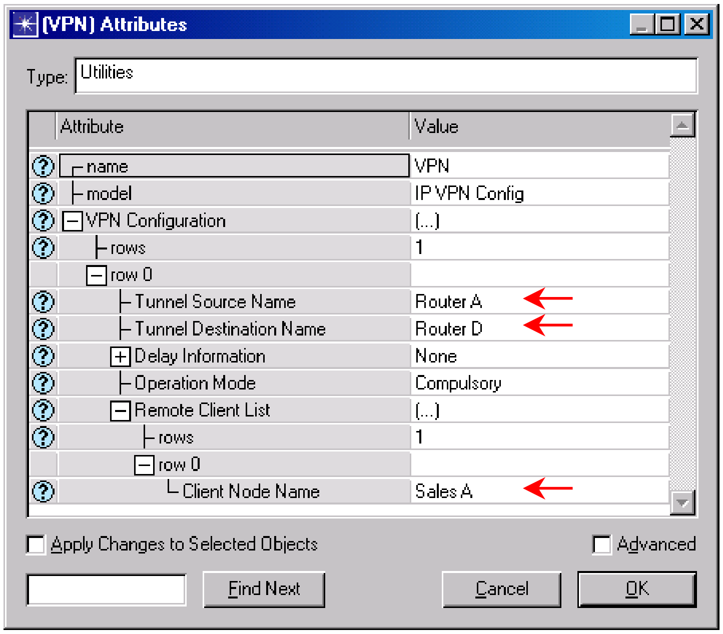
1. **Right** click on the **VPN** node ⇒ **Edit Attributes**

   i. Expand the **VPN Configuration** hierarchy ⇒ Add **one row** ⇒ Expand **row 0** hierarchy ⇒ Assign **Router A** to **Tunnel Source Name** ⇒ Assign **Router D** to **Tunnel Destination Name**.

   ii. Expand the **Remote Client List** hierarchy ⇒ Add **one row** ⇒ Expand **row 0** hierarchy ⇒ Assign **Sales A** to **Client Node Name**.

   iii. Click **OK**.

2. **Save** your project.



Type: Utilities

Attribute	Value
name	VPN
model	IP VPN Config
⊟ VPN Configuration	(...)
rows	1
⊟ row 0	
Tunnel Source Name	Router A
Tunnel Destination Name	Router D
⊞ Delay Information	None
Operation Mode	Compulsory
⊟ Remote Client List	(...)
rows	1
⊟ row 0	
Client Node Name	Sales A

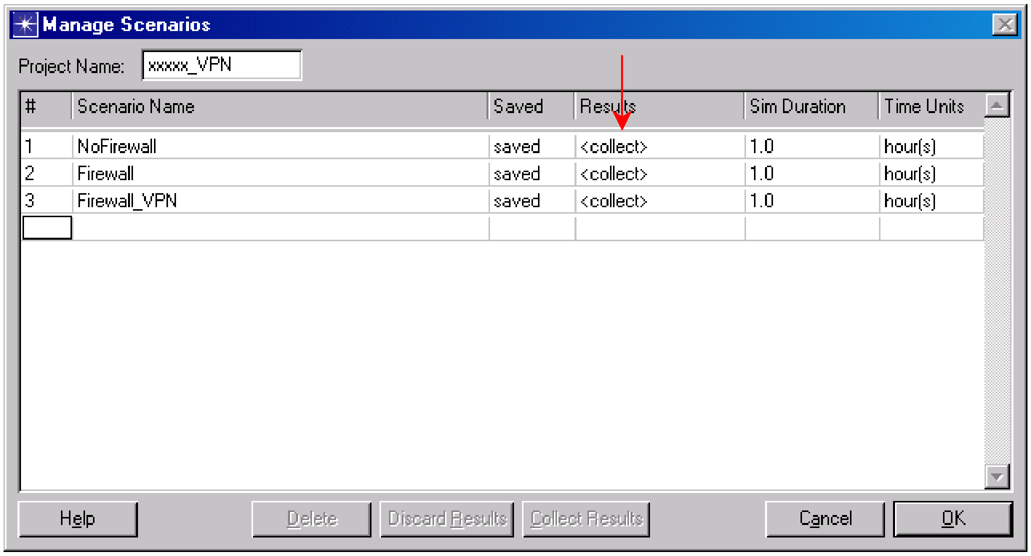
□ Apply Changes to Selected Objects □ Advanced

Run the Simulation

To run the simulation for the three scenarios simultaneously:

1. Go to the **Scenarios** menu ⇒ Select **Manage Scenarios**.

2. Change the values under the **Results** column `<collect>` (or `<recollect>`) for the three scenarios. Keep the default value of the *Simulation Duration* (1 hour). Compare to the following figure.



Project Name: xxxxx_VPN

#	Scenario Name	Saved	Results	Sim Duration	Time Units
1	NoFirewall	saved	<collect>	1.0	hour(s)
2	Firewall	saved	<collect>	1.0	hour(s)
3	Firewall_VPN	saved	<collect>	1.0	hour(s)

3. Click **OK**.

4. After the simulation complete the 3 runs, one for each scenario, click **Close**.

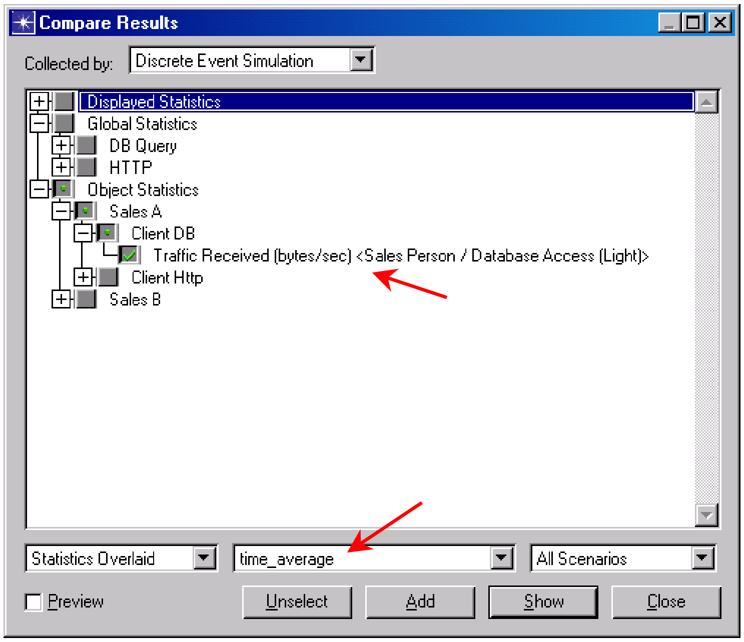
View Results

To view and analyze the results:

1. Select **Compare Results** from the **Results** menu.

2. Expand the **Sales A** hierarchy ⇒ Expand the **Client DB** hierarchy ⇒ Select the **Traffic Received** statistic.

3. Change the drop-down menu in the middle-lower part of the **Compare Results** dialogue box from **As Is** to **time_average** as shown.



Compare Results

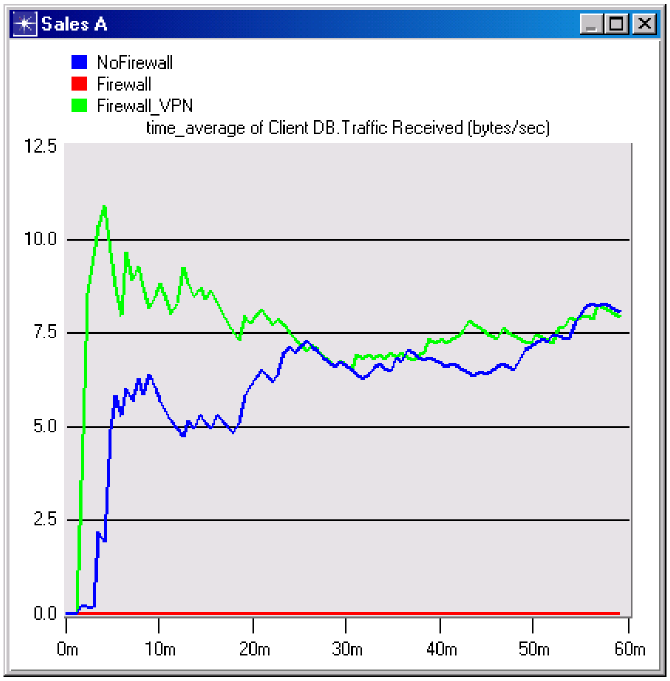
Collected by: Discrete Event Simulation

```
⊞ Displayed Statistics
⊟ Global Statistics
   ⊞ DB Query
   ⊞ HTTP
⊟ Object Statistics
   ⊟ Sales A
      ⊟ Client DB
         └ ☑ Traffic Received (bytes/sec) <Sales Person / Database Access (Light)>
      ⊞ Client Http
   ⊞ Sales B
```

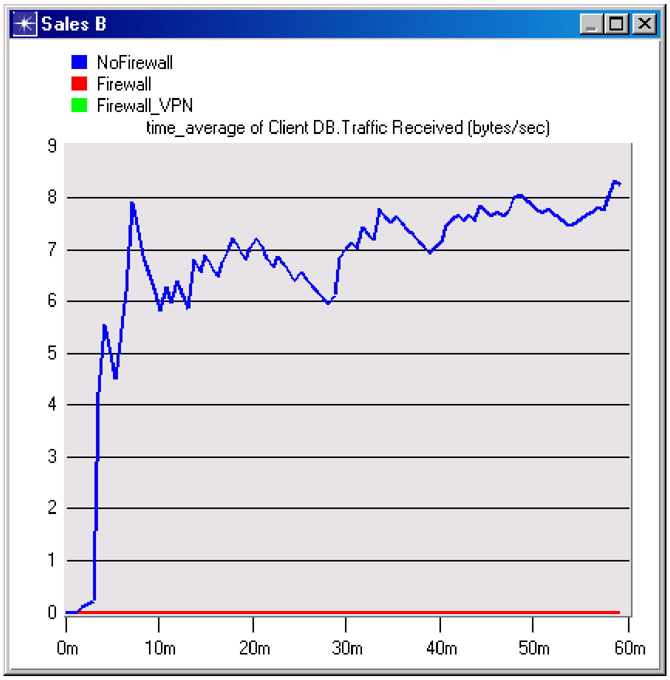
Statistics Overlaid | time_average | All Scenarios

□ Preview

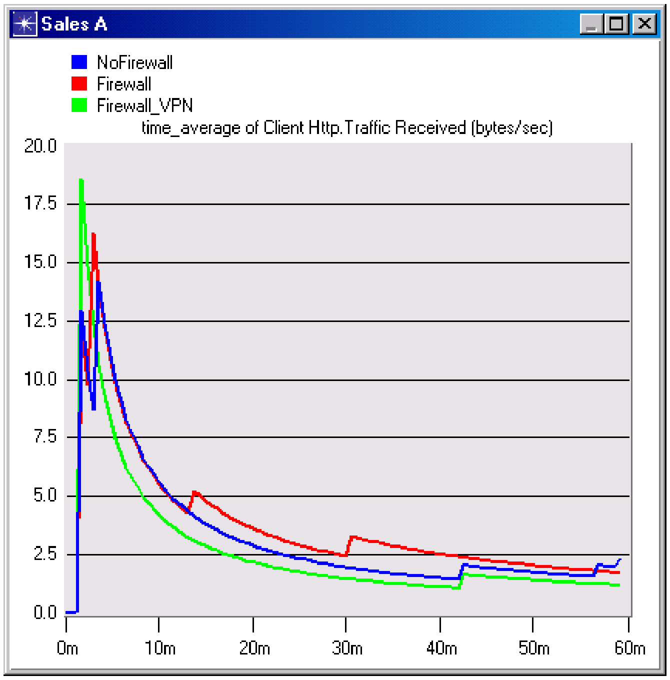
4. Press **Show** and the resulted graph should resemble the following one:

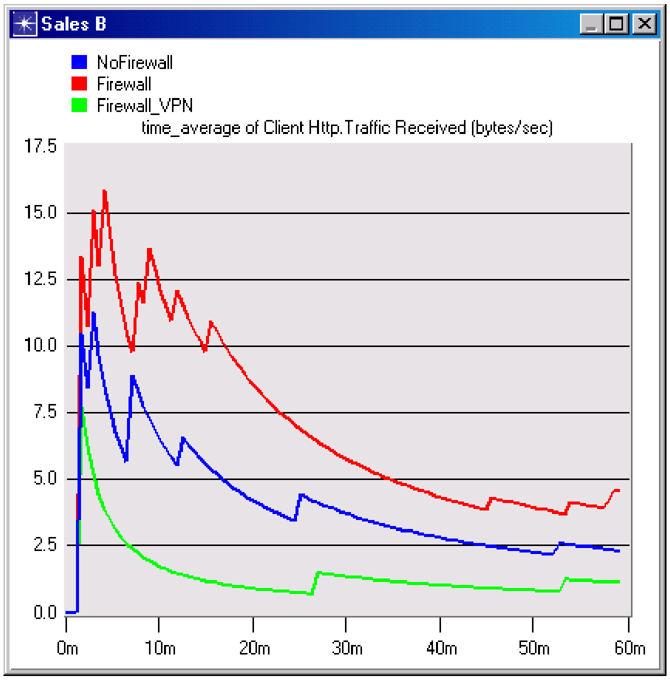


5. Create a graph similar to the previous one but for Sales B:



6. Create two graphs similar to the previous ones to depict the Traffic Received by the **Client HTTP** for **Sales A** and **Sales B**.





Hints

-

Questions

1) From the obtained graphs explain the effect of the firewall as well as the configured VPN on the database traffic requested by Sales A and Sales B.

2) Compare the graphs that show the received HTTP traffic with those that show the received Database traffic.

3) Generate and analyze the graph(s) that show the effect of the firewall as well as the configured VPN on the response time (delay) of the HTTP pages and Database queries.

4) Configure the firewall and create the necessary VPNs so that only the two sales sites, Sales A and Sales B, are allowed to browse the web sites stored in the Server.

Lab Report

Prepare a report that includes the answer to the above questions as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.