LAB 13

Firewalls and VPN

Network Security and Virtual Private Networks

OBJECTIVES

The objective of this lab is to study the role of firewalls and virtual private networks (VPNs) in providing security to shared public networks 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 application users would prefer that others not be able to read it.

A firewall router 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 characterizes the packets they will and will not forward.

A VPN is an example of providing a controlled connectivity over a public network such as the Internet. VPNs utilize a concept called an IP tunnel—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 of 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, whereas the source address is 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.

PRE-LAB ACTIVITIES

Read Sections 4.3.3 and 8.4.2 from *Computer Networks: A Systems Approach, 5th Edition*.

PROCEDURE

Create a New Project

1. Start **OPNET IT Guru Academic Edition** → Choose **New** from the **File** menu.
2. Select **Project** and click **OK** → Name the project **<your initials>_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**.

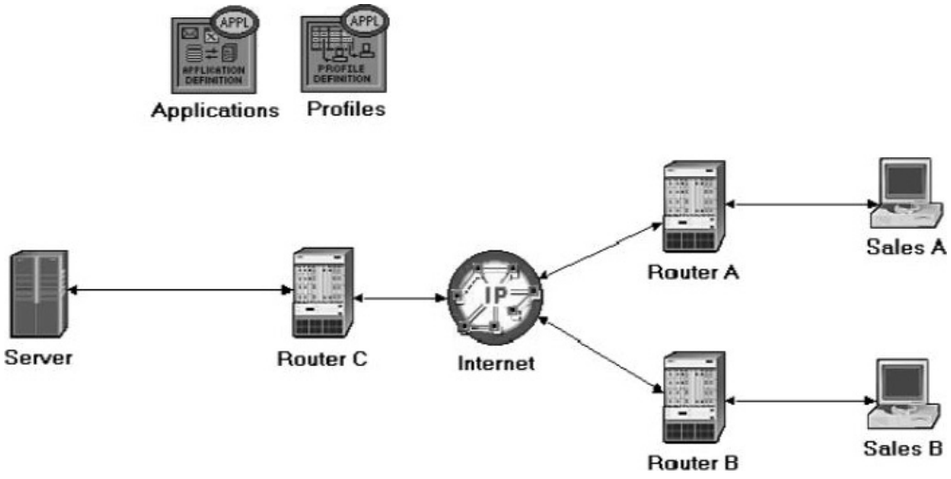
Create and Configure the Network

Initialize the network:

1. Open the *Object Palette* dialog box by clicking . Make sure that the **internet_toolbox** item is selected from the pull-down menu on the object palette.
2. Add the following objects from the palette to the project workspace (see the following figure for placement): **Application Config**, **Profile Config**, an **ip32_cloud**, one **ppp_server**, three **ethernet4_slip8_gtwy** routers, and two **ppp_wkstn** hosts.
3. Rename the objects you added and connect them using **PPP_DS1** links, as shown here:

The **ppp_server** and **ppp_wkstn** support one underlying Serial Line Internet Protocol (SLIP) connection at a selectable data rate.

PPP_DS1 connects two nodes running PPP. Its data rate is 1.544 Mbps.



Configure the nodes:

Several example application configurations are available under the **Default** setting. For example, "Web Browsing (Heavy HTTP1.1)" indicates a Web browsing application performing heavy browsing using HTTP1.1 protocol.

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).
   a. Right-click on the **Sales A** node → **Edit Attributes** → Check the **Apply Changes to Selected Objects** check-box.
   b. Expand the **Application: Supported Profiles** attribute → Set **rows** to 1 → Expand the **row 0** hierarchy → **Profile Name** = **Sales Person** (this is one of the "sample profiles" we configured in the **Profiles** node).
5. Click **OK**, and **Save** your project.

Choose the 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 box, check the following statistics:
   a. **Global Statistics → DB Query → Response Time (sec)**.
   b. **Global Statistics → HTTP → Page Response Time (seconds)**.
3. Click **OK**.
4. Right-click on **Sales A** node, and select **Choose Individual Statistics** from the menu. In the *Choose Results* dialog box, check the following statistics:
   a. **Client DB → Traffic Received (bytes/sec)**.
   b. **Client Http → Traffic Received (bytes/sec)**.
5. Click **OK**.
6. Right-click on the **Sales B** node, and select **Choose Individual Statistics** from the pop up menu. In the *Choose Results* dialog box, check the following statistics:
   a. **Client DB → Traffic Received (bytes/sec)**.
   b. **Client Http → Traffic Received (bytes/sec)**.
7. Click **OK**, and **Save** your project.

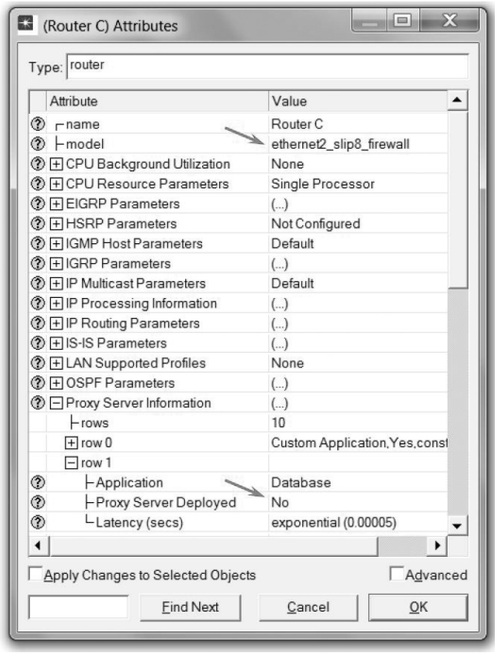
DQ Query Response Time is measured from the time when the database query application sends a request to the server to the time it receives a response packet.

HTTP Page Response Time specifies the time required to retrieve the entire page with all the contained inline objects.

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 salespeople. One way to do that is to replace Router C with a firewall as follows:

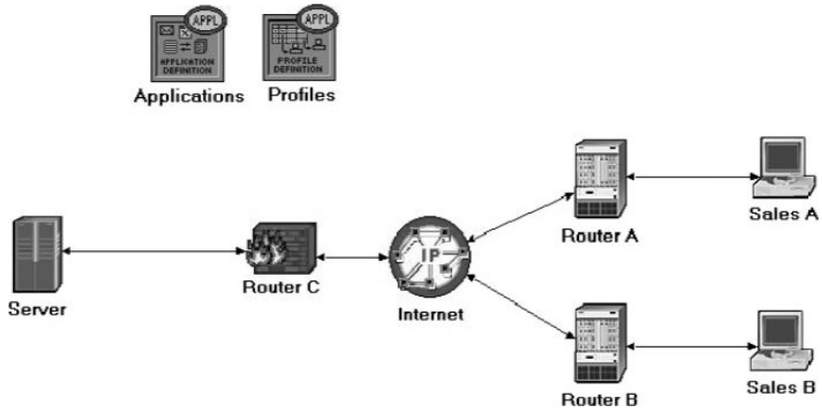
1. Select **Duplicate Scenario** from the **Scenarios** menu and name it **Firewall** → Click **OK**.
2. In the new scenario, right-click on **Router C → Edit Attributes**.
3. Assign **ethernet2_slip8_firewall** to the **model** attribute.
4. Expand the hierarchy of the **Proxy Server Information** attribute → Expand the **row 1**, which is for the database application hierarchy → Assign **No** to the **Proxy Server Deployed** attribute as shown:



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

Proxy Server Information is a table defining the configuration of the proxy servers on the firewall. Each row indicates whether a proxy server exists for a certain application and the amount of additional delay that will be introduced to each forwarded packet of that application by the proxy server.

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

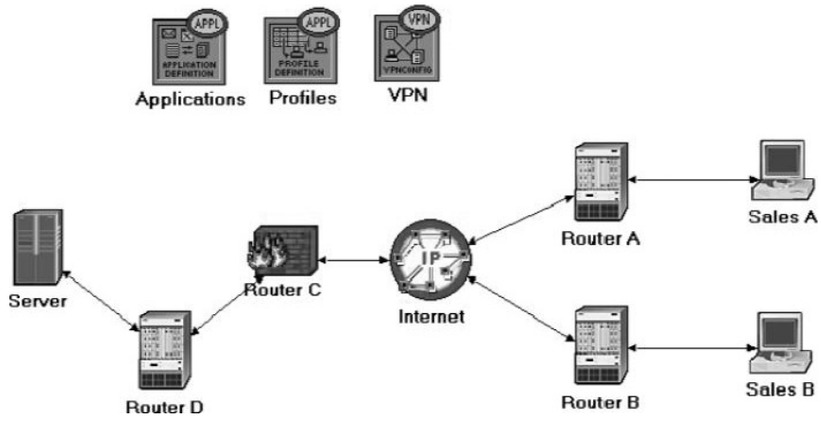


The Firewall_VPN Scenario

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 people in the **Sales A** site to have access to the databases in the server. Because 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.

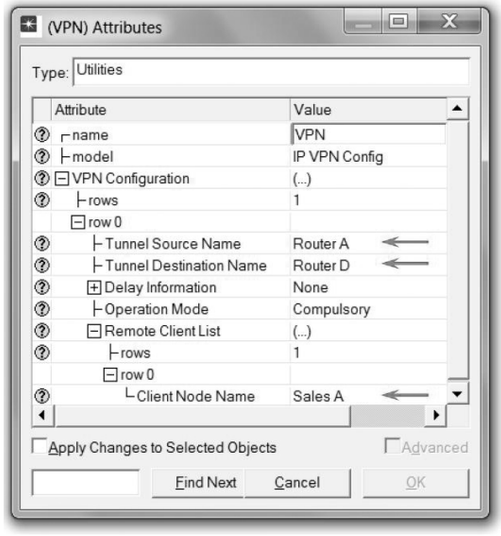
1. While you are in the **Firewall** scenario, select **Duplicate Scenario** from the **Scenarios** menu and give it the name **Firewall_VPN** → Click **OK**.
2. Remove the link between **Router C** and the **Server**.
3. Open the *Object Palette* dialog box by clicking . Make sure that the **internet_toolbox** is selected from the pull-down menu on the object palette.
   a. Add to the project workspace one **ethernet4_slip8_gtwy** and one **IP VPN Config** (see the following figure for placement).
   b. From the *Object palette,* use two **PPP_DS1** links to connect the new router to the **Router C** (the firewall) and to the **Server**, as shown in the following figure.
   c. Close the *Object Palette* dialog box.
4. Rename the **IP VPN Config** object to **VPN**.
5. Rename the new router to **Router D** as shown in the following figure:

The **ethernet4_slip8_gtwy** node model represents an IP-based gateway supporting four Ethernet hub interfaces and eight serial line interfaces. IP packets arriving on any interface are routed to the appropriate output interface based on their destination IP address. The Routing Information Protocol (RIP) or the Open Shortest Path First (OSPF) protocol may be used to dynamically and automatically create the gateway's routing tables and select routes in an adaptive manner.



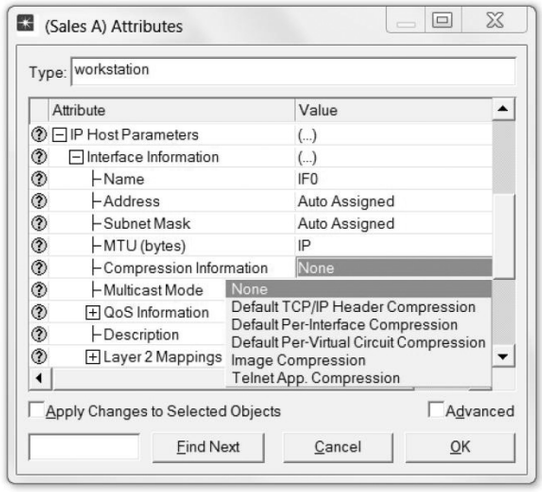
Configure the VPN:

1. Right-click on the **VPN** node → **Edit Attributes**.
   a. Expand the **VPN Configuration** hierarchy → Set **rows** to **1** → Expand **row 0** hierarchy → Edit the value of **Tunnel Source Name** and enter **Router A** → Edit the value of **Tunnel Destination Name** and enter **Router D**.
   b. Expand the **Remote Client List** hierarchy → Set **rows** to **1** → Expand **row 0** hierarchy → Edit the value of **Client Node Name** and enter **Sales A**.
   c. Click **OK**, and **Save** your project.



Simulating encryption:

A virtual tunnel between the **Sales A** and the **Server** does not guarantee security for the contents of the transferred database packets. If the contents of these packets are confidential, encryption of these packets will be needed. In OPNET AE, the effect of packet encryption can be simulated by the available compression function. Two of the available compression schemes are the Per-Interface Compression and the Per-Virtual Circuit Compression, as shown in the following figure. Once you edit the Compression Information attribute of an interface, OPNET adds the IP Config node to the project.

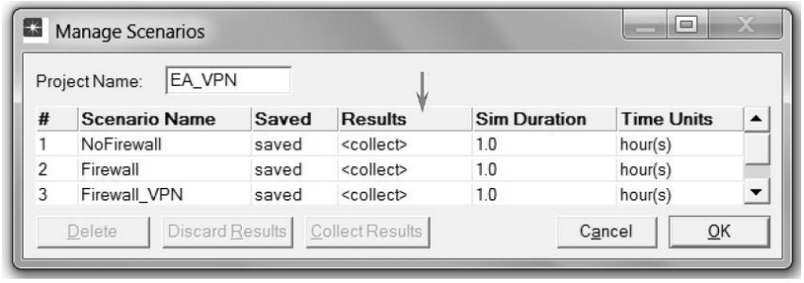


Per-Interface Compression compresses the entire packet (including the headers). This means the packet is decompressed and compressed at each hop on the route. Per-Virtual Circuit Compression compresses the packet payload only. Therefore, compression and decompression take place only at the end nodes. One of the exercises at the end of this lab requires you to create a new scenario to utilize the compression function.

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 to **<collect>** (or **<recollect>**) for the three scenarios. Keep the default value of the **Sim Duration** (1 hour). Compare with the following figure.

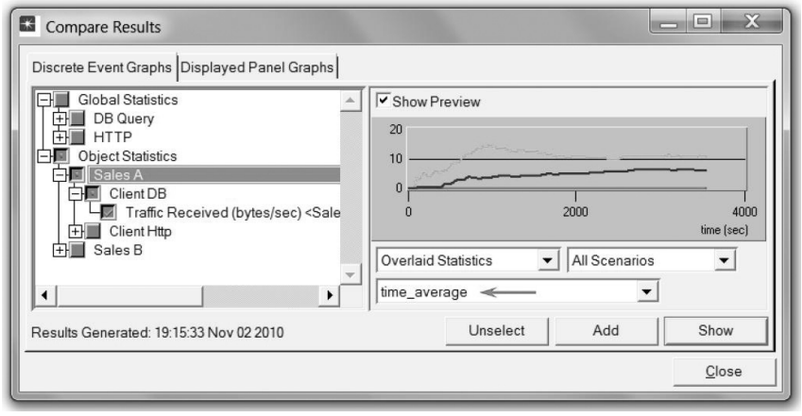


3. Click **OK** to run the three simulations. Depending on the speed of your processor, this task may take several seconds to complete.
4. After the three simulation runs complete, one for each scenario, click **Close**.

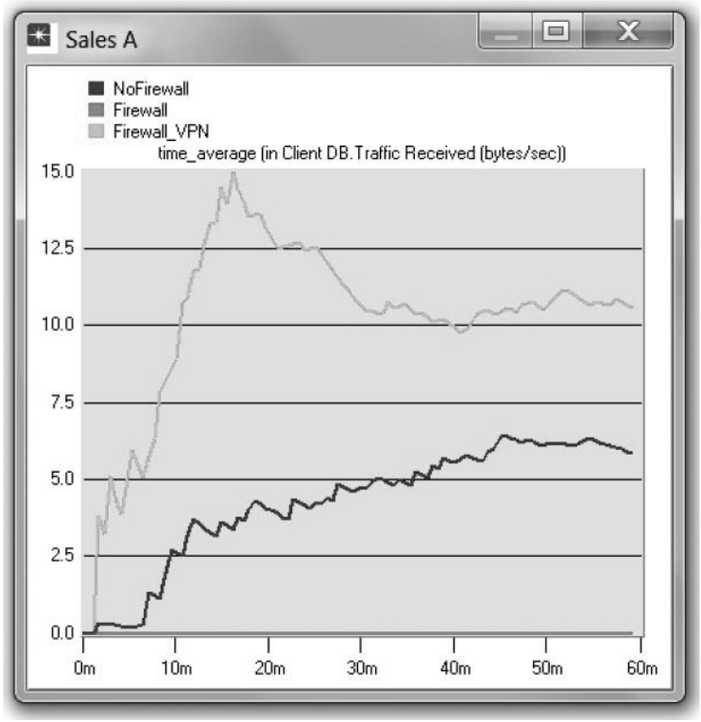
View the Results

To view and analyze the results:

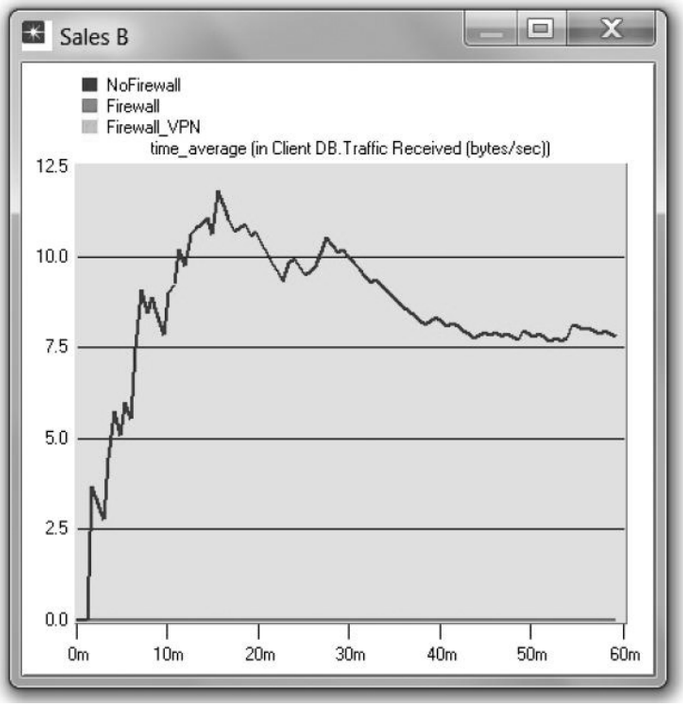
1. Select **Compare Results** from the **Results** menu.
2. Expand the **Sales A** hierarchy → Expand the **Client DB** hierarchy → Select the **Traffic Received** statistic.
3. Change the drop-down menu in the middle-lower part of the *Compare Results* dialog box from **As Is** to **time_average** as shown.



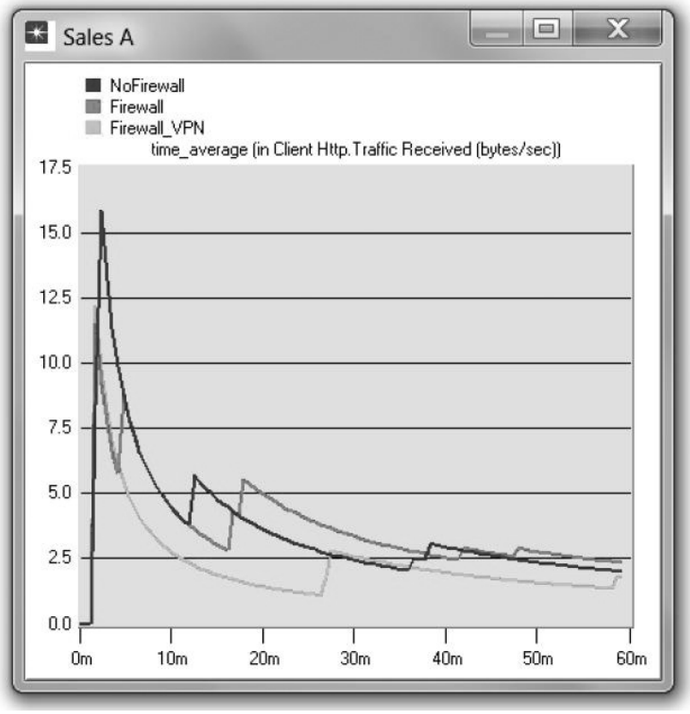
4. Press **Show** and the resulting graph should resemble the following figure. Your graph may not match exactly because of node placement.



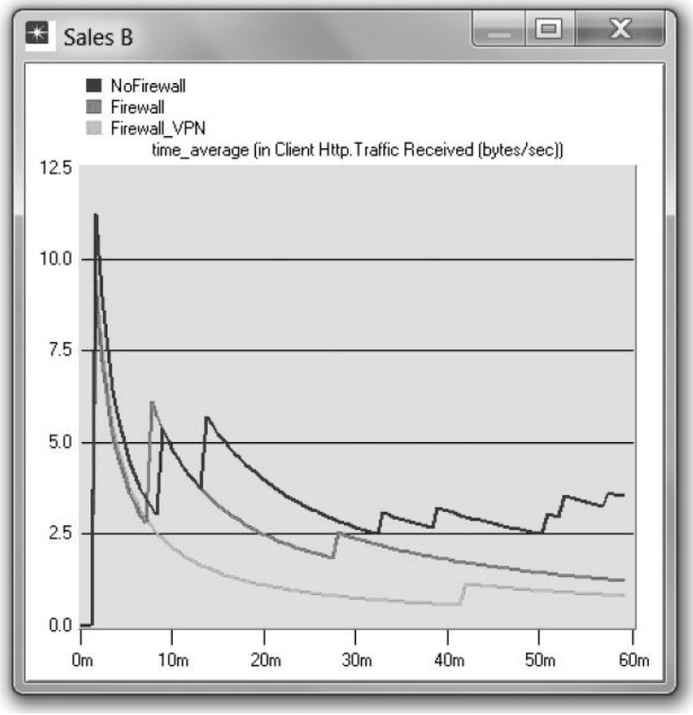
5. Create a graph similar to the previous one, but for **Sales B**:



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



Note: Results may vary slightly because of different node placement.



FURTHER READINGS

The Impact of Internet Link Capacity on Application Performance: From the **Protocols** menu, select **Methodologies → Capacity Planning**.

Virtual Private Networks: IETF RFC number 2685 (www.ietf.org/rfc.html).

EXERCISES

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. In the **Firewall_VPN** scenario, we configured the **VPN** node so that no traffic from **Sales A** is blocked by the firewall. Create a duplicate of the **Firewall_VPN** scenario, and name the new scenario **Q4_DB_Web**. In the **Q4_DB_Web** scenario, we want to configure the network so that:
   a. The databases in the server can be accessed *only* by the people in the **Sales A** site.
   b. The Web sites in the server can be accessed *only* by the people in the **Sales B** site.
   Include in your report the diagram of the new network configuration, including any changes you made to the attributes of the existing or added nodes. Generate the graphs of the DB traffic received and the HTTP traffic received for both **Sales A** and **Sales B**, to show that the new network meets the previously mentioned requirements.
5. Create a duplicate of the **Firewall_VPN** scenario, and name the new scenario **Q5_Compression**. In the new scenario, simulate packet encryption between **Sales A** and the **Server** by allowing **Per-Virtual Circuit Compression** in both nodes. Because encryption takes more time than compression, edit the attributes of the Per-Virtual Circuit Compression row (row 3) in the **IP Config** node. Assign 3E-006 and 1E-006 to **Compression Delay** and **Decompression Delay**, respectively. Study the effect of compression on the DB Query response time between **Sales A** and the **Server**.

LAB REPORT

Prepare a report that follows the guidelines explained in the Introduction Lab. The report should include the answers to the preceding exercises 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.