

TP4

FIREWALLS ET VPN

SECURITE RESEAUX ET VIRTUAL PRIVATE NETWORK

À rendre le mercredi 18 janvier 2006

1. INTRODUCTION

Le but de ce travail pratique est de comprendre et d'analyser le fonctionnement des *firewalls* et des *Virtual Private Networks* (VPNs). Ces derniers mettent en œuvre des mécanismes de sécurité dans les réseaux publics.

2. MONTAGE ET CONFIGURATION DU RESEAU

Un réseau sera monté modélisant d'un côté un serveur et de l'autre des clients, étant tous connectés à travers l'Internet. Le serveur offrira les applications suivantes : accès distante à une base de données, serveur email et serveur web. On modélisera deux clients nommés *Sales A* et *Sales B* qui se connecteront au serveur pour utiliser les services offerts.

Trois scénarios seront montés. Le premier implémentera le réseau décrit précédemment. Le deuxième scénario, nommé *Firewall*, remplacera le routeur du serveur par un *firewall* pour ainsi éviter l'accès à la base de données depuis l'extérieur. En fin, le troisième établira un VPN entre le serveur et le client *Sales A* pour lui accorder un accès à la base de données malgré la présence du *firewall*.


Création d'un nouveau projet

Créez un nouveau projet ayant les caractéristiques suivantes :

Attribut	Valeur
Project Name	<login1> <login2> tp4_Firewalls_VPN
Scenario Name	NoFirewall
Initial Topology	Create Empty Scenario
Network Scale	Logical

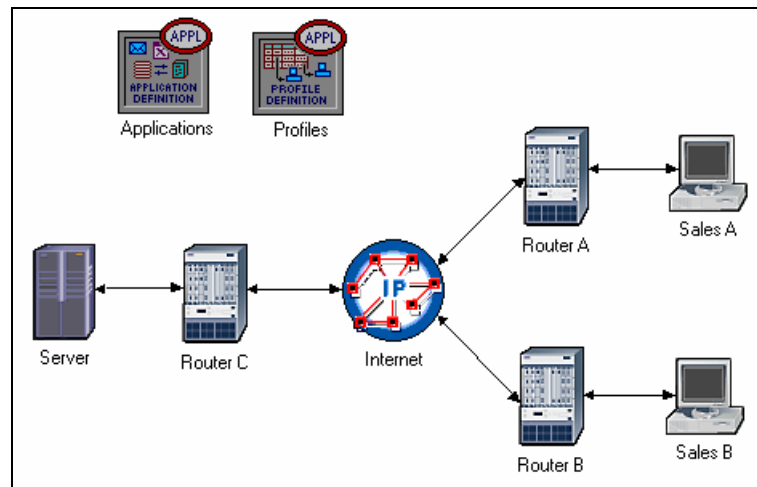
Montage du réseau

Les composants dont vous avez besoin pour monter les réseaux sont décrits ci-dessous.

Souvenez-vous que pour les utiliser il faut cliquer sur l'icône Palette  et choisir la palette dans le menu déroulant.

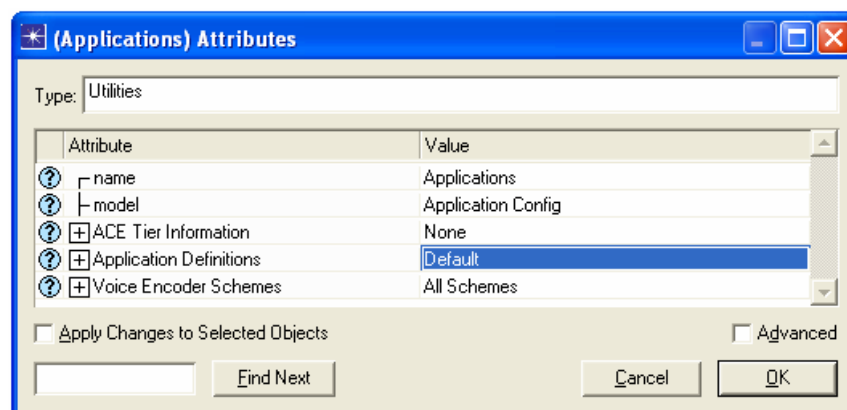
Quantité	Composant	Palette	Description
3	ethernet4_slip8_gtwy	internet_toolbox	Routeurs
1	ip32_cloud	internet_toolbox	Abstraction de l'Internet
6	PPP_DS1	internet_toolbox	Connexions entre les différents noeuds
1	ppp_server	internet_toolbox	Serveur
2	ppp_wkstn	internet_toolbox	Clients
1	Application Config	internet_toolbox	Configurer les applications : HTML, FTP, Database, Email, etc.
1	Profile Config	internet_toolbox	Configurer les profils : Application utilisées par un client

À l'aide des composants précédents, montez le réseau de sorte qu'il se ressemble à celui de la figure ci-dessous :

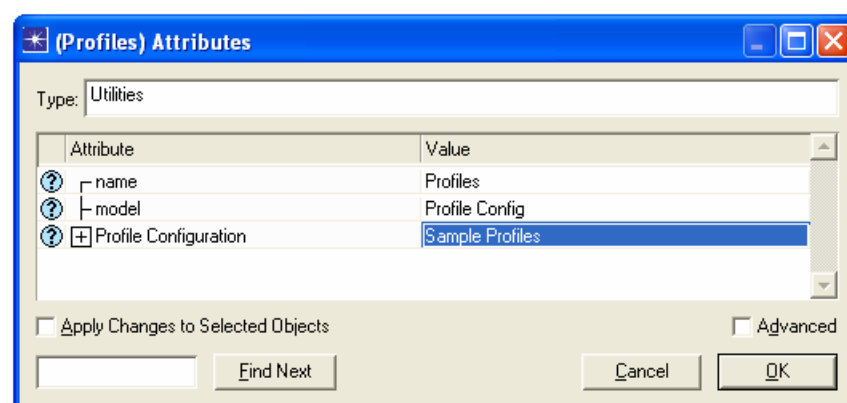


Configuration des nœuds

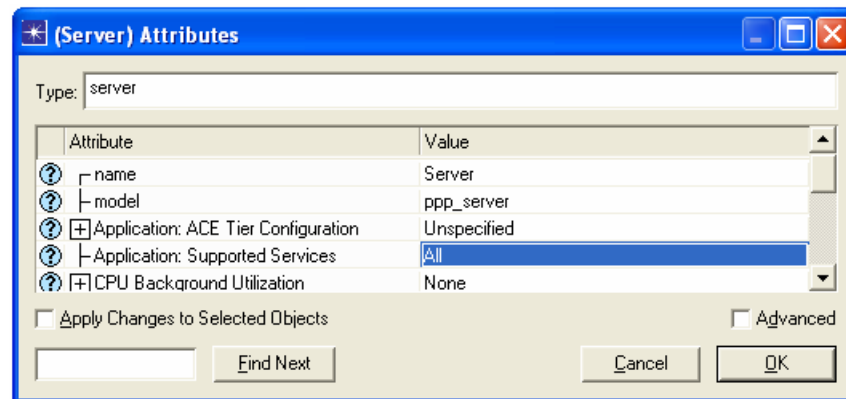
1. Cliquez droit sur le nœud **Applications** → **Edit Attributes** → Assignez la valeur **Default** à l'attribut **Application Definitions** → Cliquez sur **OK**.



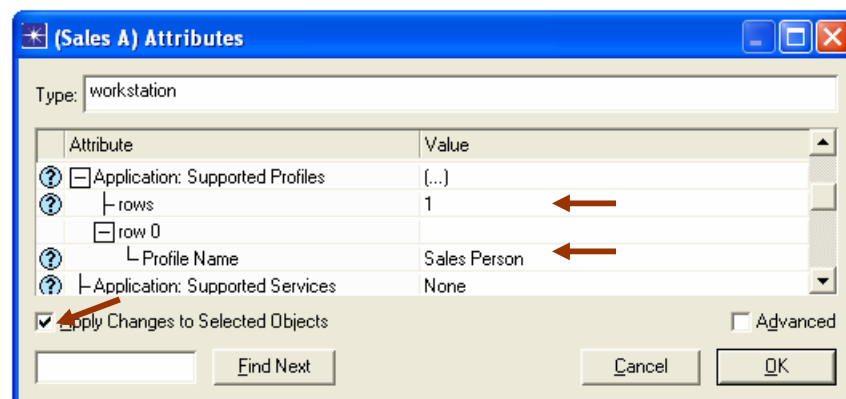
2. Cliquez droit sur le nœud **Profiles** → **Edit Attributes** → Assignez la valeur **Sample Profiles** à l'attribut **Profile Configuration** → Cliquez sur **OK**.



3. Cliquez droite sur le nœud **Server** → **Edit Attributes** → Assignez la valeur **All** à l'attribut **Application : Supported Services** → Cliquez sur **OK**.



4. Cliquez droit sur le nœud **Sales A** → **Select Similar Nodes** (assurez-vous que les nœuds **Sales A** et **Sales B** soient sélectionnés)
 - a. Cliquez droit sur le nœud **Sales A** → **Edit Attributes** → Cochez la case **Apply Changes to Selected Objects**.
 - b. Ajoutez une ligne à l'attribut **Applications : Supported Profiles** (assignez la valeur 1 au lieu de 0) → Dépliez la hiérarchie de **row 0** → Assignez la valeur **Sales Person** à l'attribut **Profile Name**.
 - c. Cliquez sur **OK**.



5. Sauvegardez votre projet.

Choix des statistiques

1. Cliquez droit sur n'importe quel endroit de l'espace de travail et choisissez **Choose Individual Statistics** dans le menu contextuel.
2. Dans la fenêtre **Choose Results**, choisissez les trois statistiques suivantes :
 - a. **Global Statistics** → **DB Query** → **Response Time (sec)**.
 - b. **Global Statistics** → **HTTP** → **Page Response Time (sec)**.
 - c. **Global Statistics** → **IP** → **Traffic Dropped (packets/sec)**.
3. Cliquez sur **OK**.
4. Cliquez droit sur le nœud **Sales A** et choisissez **Choose Individual Statistics** dans le menu contextuel.
5. Dans la fenêtre **Choose Results**, choisissez les trois statistiques suivantes :
 - a. **Node Statistics** → **Client DB** → **Traffic Received (bytes/sec)**.
 - b. **Node Statistics** → **Client HTTP** → **Traffic Received (bytes/sec)**.

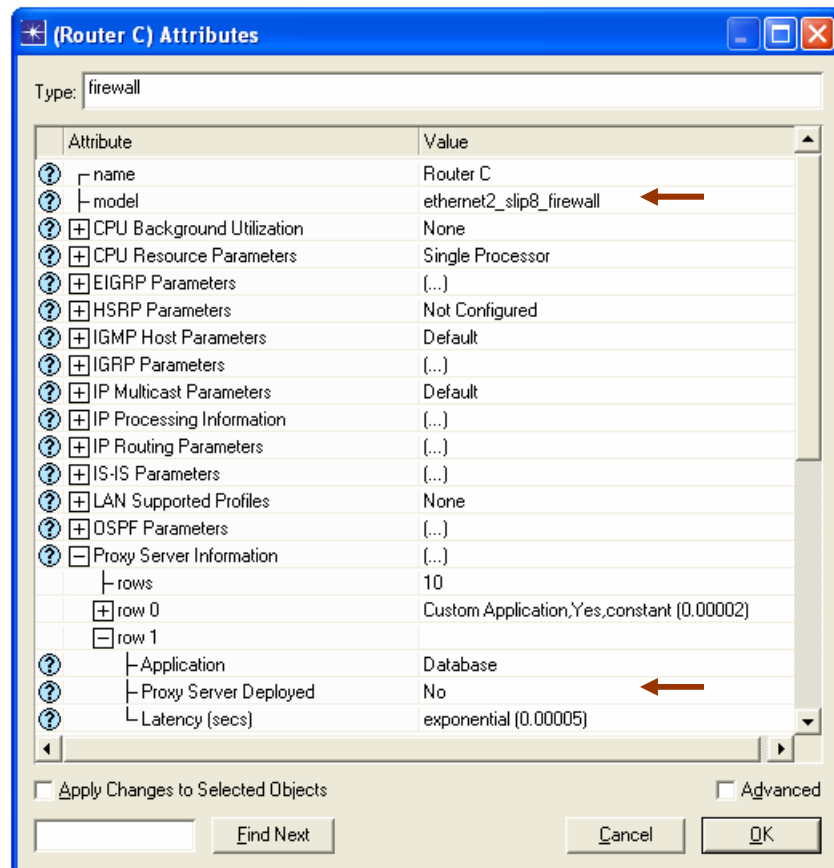
6. Cliquez sur **OK**.
7. Cliquez droit sur le nœud **Sales B** et choisissez **Choose Individual Statistics** dans le menu contextuel.
8. Dans la fenêtre **Choose Results**, choisissez les trois statistiques suivantes :
 - a. **Node Statistics** → **Client DB** → **Traffic Received (bytes/sec)**.
 - b. **Node Statistics** → **Client HTTP** → **Traffic Received (bytes/sec)**.
9. Cliquez sur **OK** et sauvegardez votre projet.

Duplication du scénario

Scénario Firewall :

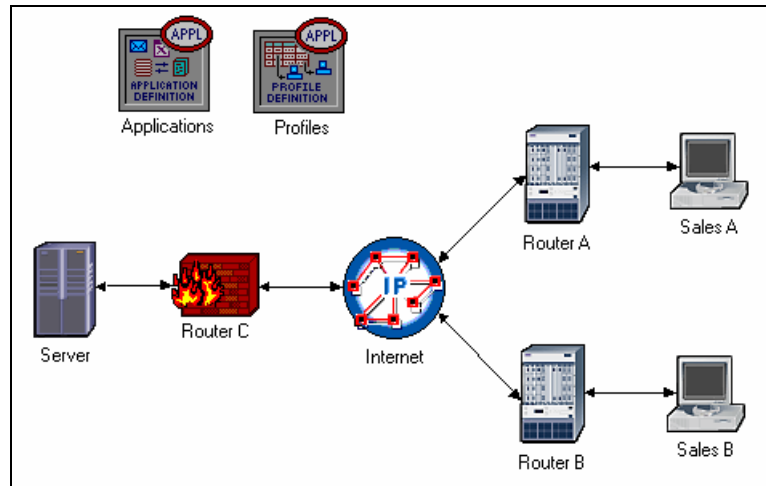
Dans le réseau précédant on a créé seulement le profile *Sales Person* qui est capable d'accéder aux applications suivantes dans le serveur : *Database Access*, *Email* et *Web Browsing* (regardez le *Profile Configuration* dans le nœud *Profile*). Supposons maintenant qu'on a besoin de protéger l'accès à la base de données du serveur (application *DataBase Access*) depuis l'extérieur, y inclus les *Sales Peron A* et *B*. Une façon d'accomplir cette tâche est d'utiliser un *Firewall* au lieu du *Router C* comme le propose ce scénario :

1. Choisissez **Duplicate Scenario** dans le menu **Scenarios** et nommez le **Firewall** → Cliquer sur **OK**.
2. Dans le nouveau scénario, choisissez **Router C** → **Edit Attributes**.
3. Assignez la valeur **ethernet2_slip8_firewall** à l'attribut **model**.
4. Dépliez la hiérarchie de l'attribut **Proxy Server Information** → Dépliez l'attribut **row 1** qui est l'application *Database* → Assignez la valeur **No** à l'attribut **Proxy Server Deployed** comme ci-dessous :



5. Cliquez sur **OK** et sauvegardez votre projet.

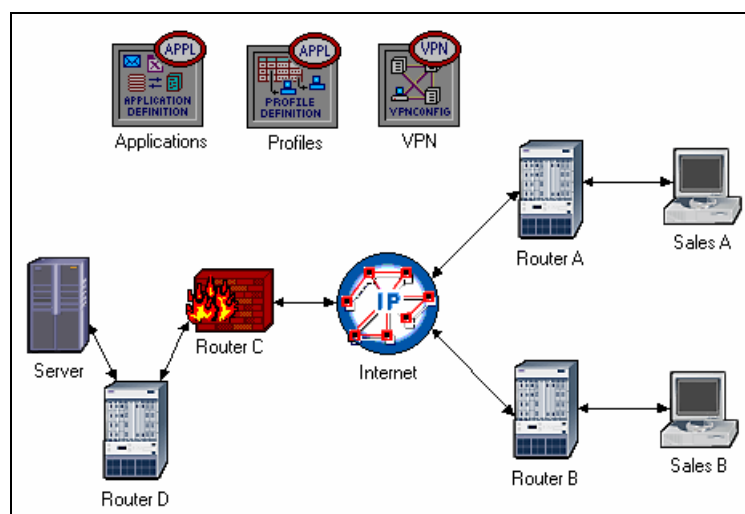
Le *Firewall* arrêtera le trafic concernant l'accès à la base de données du serveur. Comme ça cette base de données sera protégée contre l'accès extérieur. Voici à quoi devrait se ressembler ce scénario :



Scénario Firewall_VPN :

Dans le réseau *Firewall*, on a protégé la base de données du serveur contre « tout » l'accès externe. Supposons maintenant qu'on veut permettre à la personne *Sales A* d'accéder à cette base de données. Étant donné que le *Firewall* filtre tout l'accès à cette base de données, on est obligé d'utiliser une VPN. Un tunnel virtuel (IP tunnel) peut être utilisé pour faire les requêtes entre *Sales A* et la base de données. Le *Firewall* ne filtrera pas ce trafic car les paquets seront encapsulés dans un IP datagramme dans le tunnel.

1. Choisissez le scénario **Firewall**.
2. Choisissez **Duplicate Scenario** dans le menu **Scenarios** et nommez le **Firewall_VPN** → Cliquez sur **OK**.
3. Modifiez-le de sorte à obtenir le scénario suivant :

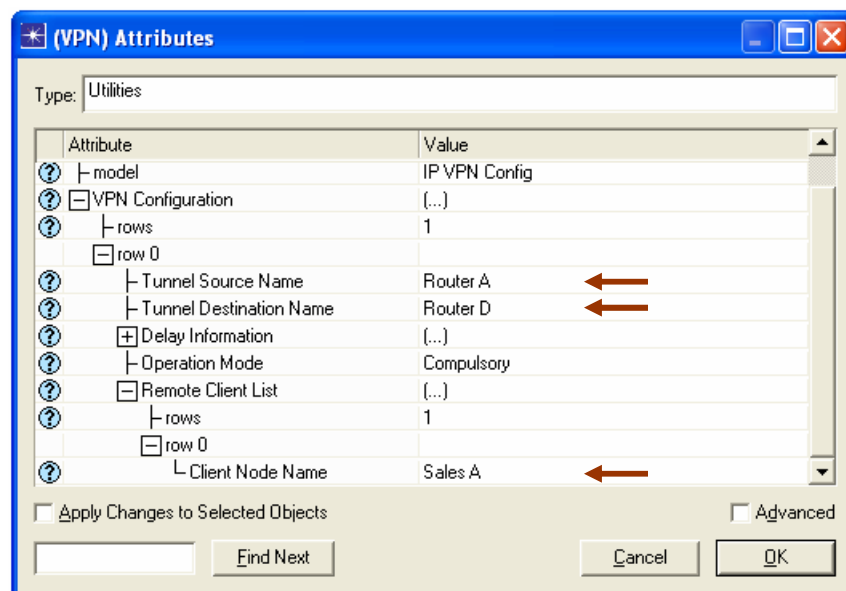


Utilisez les composants suivants pour le modifier :

Quantité	Composant	Palette	Description
1	ethernet4_slip8_gtwy	internet_toolbox	Routeurs
2	PPP_DS1	internet_toolbox	Connexions entre les différents noeuds
1	IP VPN Config	internet_toolbox	Configurer le VPN

Configuration du VPN :

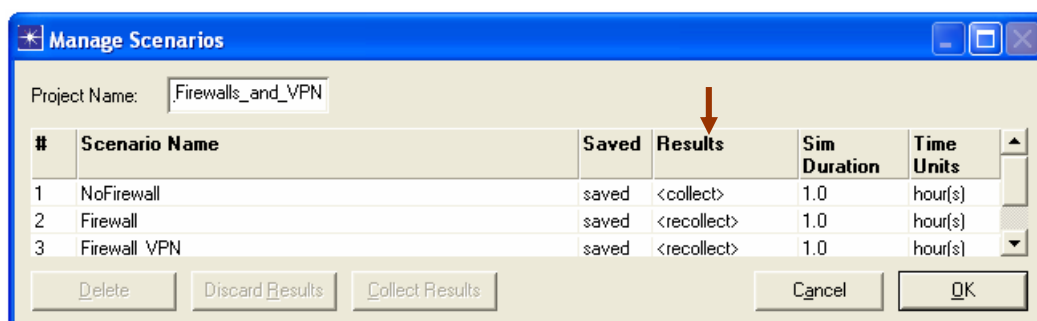
1. Cliquez droit sur le nœud **VPN** → **Edit Attributes**.
 - a. Dépliez la hiérarchie de l'attribut **VPN Configuration** → Ajoutez une ligne → Dépliez la hiérarchie de **row 0** → Assignez la valeur **Router A** à l'attribut **Tunnel Source Name** → Assignez la valeur **Router D** à l'attribut **Tunnel Destination Name**.
 - b. Dépliez la hiérarchie de l'attribut **Remote Client List** → Ajoutez une ligne → Dépliez la hiérarchie de **row 0** → Assignez **Sales A** à l'attribut **Client Node Name**.
 - c. Cliquez sur **OK**.
2. Sauvegardez votre projet.



Simulation

Pour démarrer la simulation dans les trois scénarios :

1. Choisissez **Manage Scenarios** dans le menu **Scenarios**.
2. Fixez les valeurs de la colonne **Results** à **<collect>** (ou **<recollect>**) pour les trois scénarios (voir la figure ci-dessous).

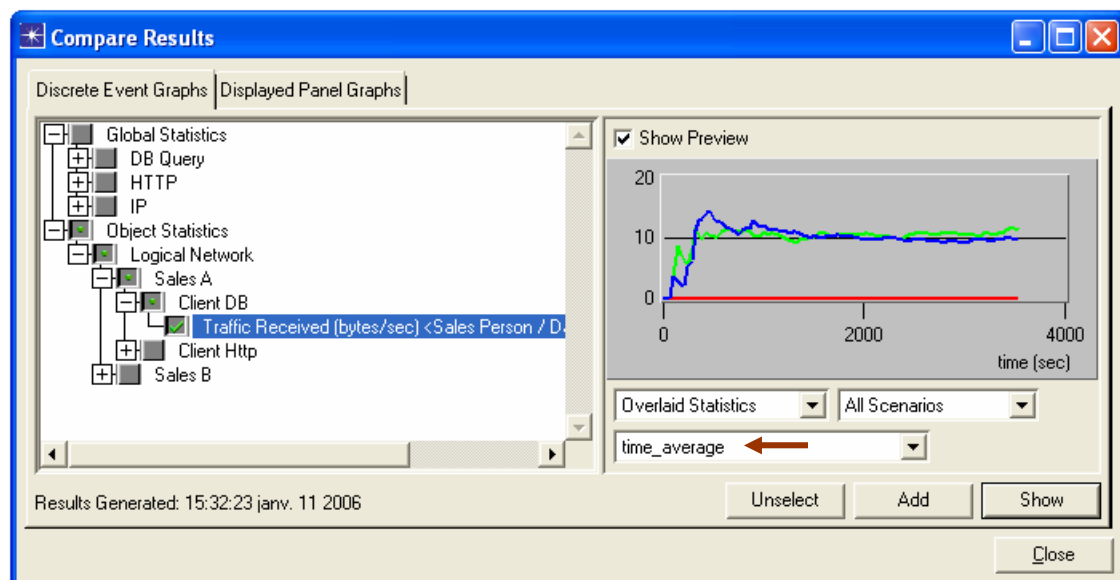


3. Cliquez sur **OK** pour démarrer les trois simulations. Le temps de simulation peut varier selon la vitesse du processeur.
4. Après que les trois simulations soient finies, une pour chaque scénario, cliquez sur **Close**.
5. Sauvegardez votre projet.

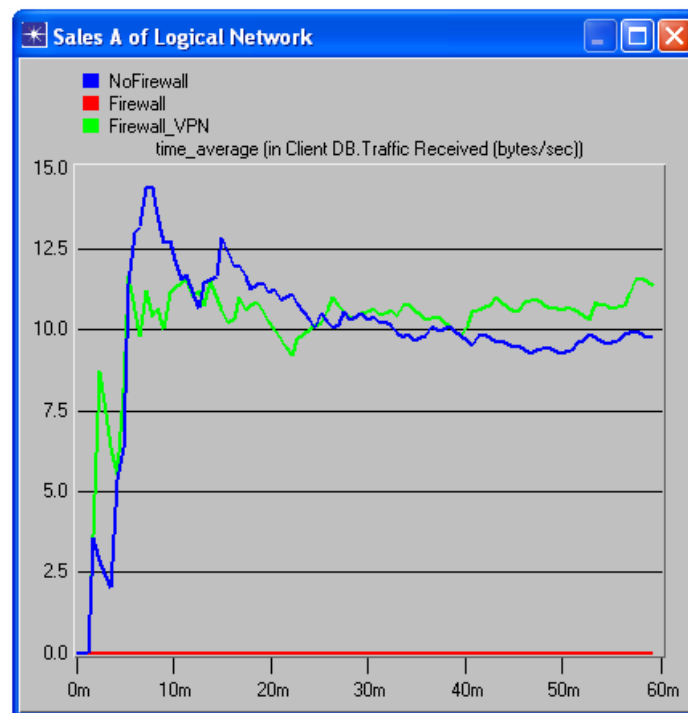
Affichage des résultats

Pour afficher et analyser les résultats :

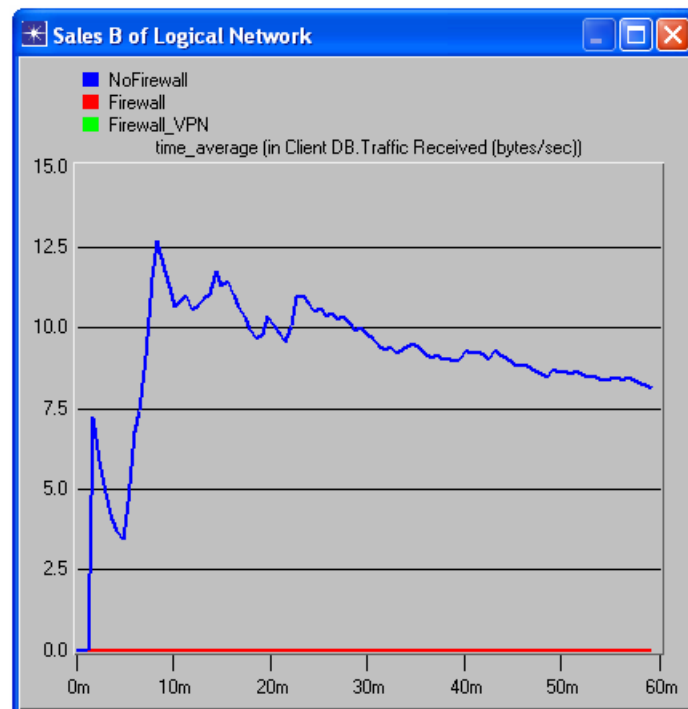
1. Choisissez l'option **Compare Results** dans le menu **Results**.
2. Dépliez la hiérarchie de **Sales A** → Dépliez la hiérarchie de **Client DB** → Sélectionnez la statistique **Traffic Received**.
3. Changez le menu déroulant de la fenêtre **Compare Results** à **time_average** au lieu de **As Is**.



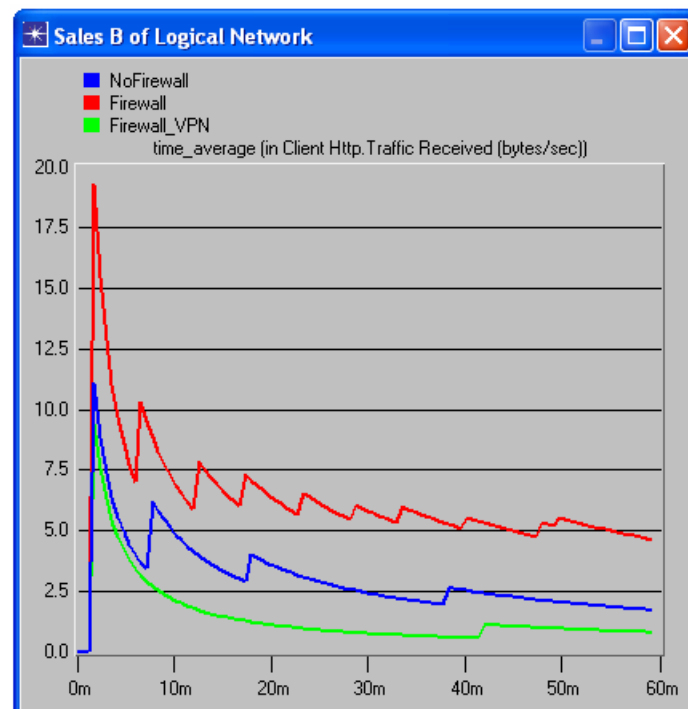
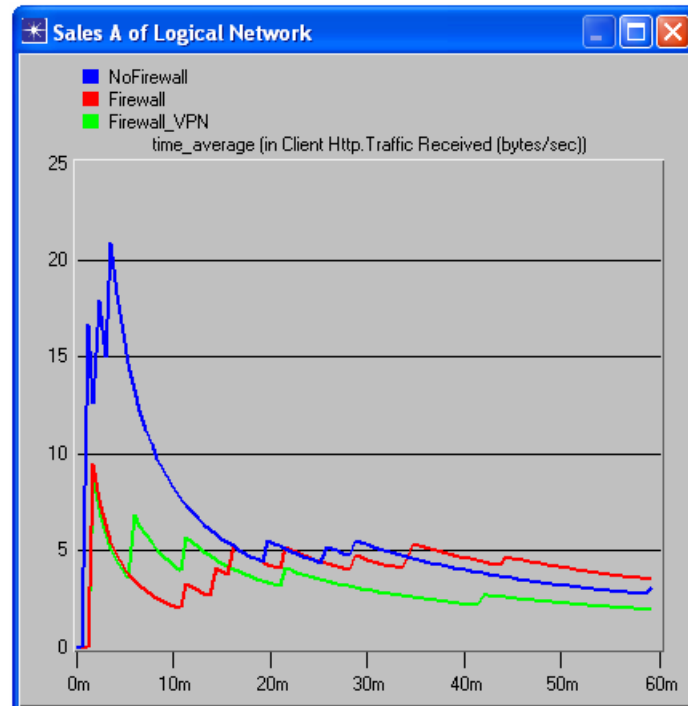
4. Cliquez sur **Show** et la graphique résultante devrait se ressembler à celle-ci :



5. Créez une graphique similaire pour **Sales B**:



6. Créez deux graphiques similaires aux précédentes pour analyser le trafic reçu par **Client http** pour les nœuds **Sales A** et **Sales B** :



3. QUESTIONS

1. À l'aide des graphiques précédentes, analysez et argumentez l'effet de l'utilisation d'un *firewall* et du VPN sur le trafic reçu concernant la base de données.
2. Analysez et comparez les graphiques du trafic reçu concernant les connexions http avec celles de l'accès à la base de données pour les deux clients *Sales A* et *Sales B*.
3. Générez, comparez et analysez les graphiques du temps de réponse (delay) des pages http et des requêtes à la base de données (générez des graphiques comparant les trois scénarios). Discutez sur l'effet du *firewall* et du VPN.
4. Générez et analysez la graphique du trafic éliminé (traffic dropped) concernant les trois scénarios. Discutez sur l'effet du *firewall* et du VPN.

4. RAPPORT

Un rapport sur papier devra être rendu contenant une description sommaire de l'implémentation des scénarios et contenant aussi des screens shots des réseaux montés. Pour chaque question (cf. § 3 Questions), les réponses doivent inclure des screens shots des graphiques et des tables résultantes ainsi qu'un analyse détaillé. Les réponses aux questions pourront aussi contenir des graphiques ou des données supplémentaires que vous considérez pertinentes.