IUT d'Angers
License Sari
Module FTA3

Compte Rendu

«Firewall et sécurité d'un réseau d'entreprise»

Par

Sylvain Lecomte

Le 07/01/2008

Sommaire

1. Introduction

Le but de ce TP 'Firewall et sécurité d'un réseau d'entreprise' est de mettre tout d'abord en place un routeur ADSL CISCO 837 conformément à la plage d'adresse fourni et routé par l'opérateur Internet. Cela nous permettras de découvrir dans un premier temps, la technologie IP ADSL et son paramétrage puis ensuite de découvrir les règles de sécurité qu'il faut mettre en œuvre pour protéger le réseau local de l'entreprise.

2. Matériels requis

Faire l'inventaire des matériels et logiciels ci-dessous :

Ressources communes :

- 1 x câble console CISCO (bleu clair, RJ45 – RS232 9pts Femelle) avec rallonge éventuelle)
- Divers : Câbles Ethernet droits et croisés de catégorie 5
- 3 x PC sous Windows ou Linux – Fedora avec couche TCP/IP installée (2 stations XP-Pro et 1 serveur 2003)
- Logiciels installés :
  - Logiciel d'émulation de terminal (mode vt100) pour le management « OUTBAND » (HyperTerminal Private Edition V 6.3)
  - PSP 6 (pour les captures d'écrans)
  - SuperScan (Scanneur de ports)
  - Sniffers : Snifmon (commercial : ufasoft) et WireShark (libre)
- 1 Texte de TP couleur relié
- Annexes

Ressources spécifiques :

TP N°4 : Firewall et sécurité d'un réseau d'entreprise

- 1 x câbles de console CISCO (RJ45 – RS232 9 pts Femelle)
- 1 x câble de liaison série (DB9F – DB9F type RS232C)
- 1 routeur CISCO 837H
- 1 x firewall WatchGuard Firebox
- 1 x commutateur CISCO C2950-12

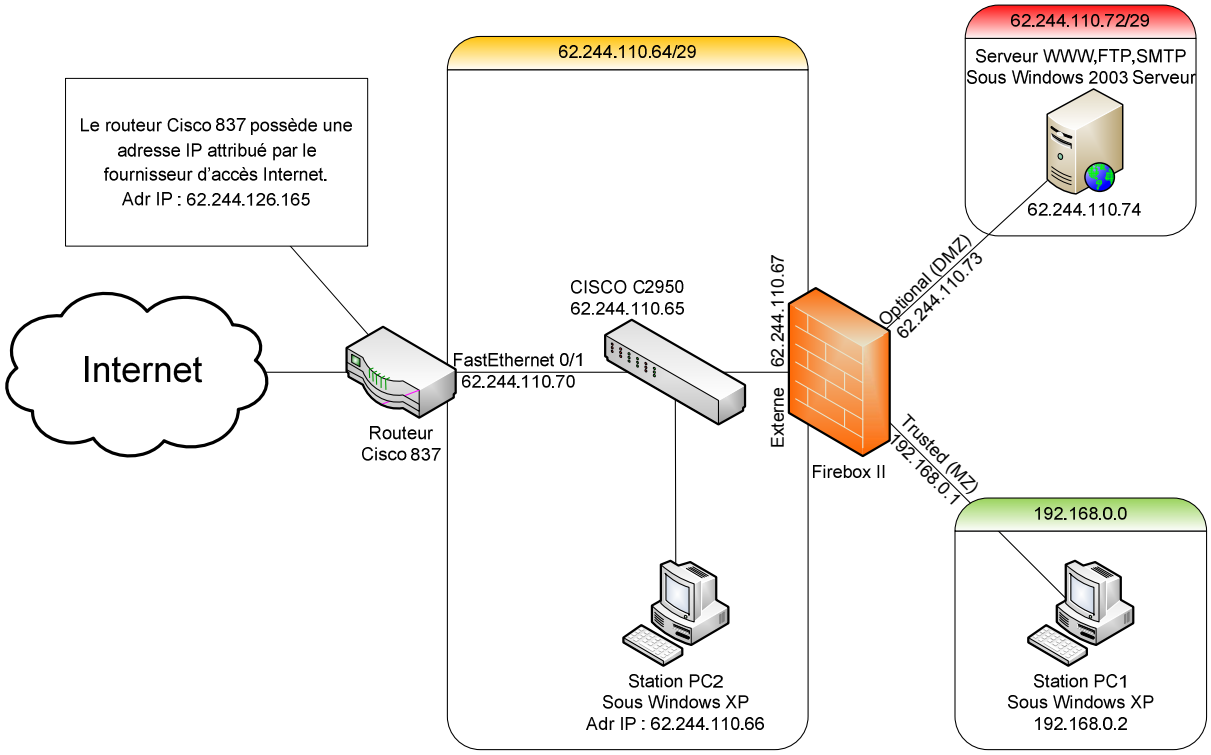
3. Mise en place d'une infrastructure réseau d'entreprise sécurisée

3.1 Objectif de la manipulation

L'objectif de la manipulation est de mettre en place l'ensemble des matériels et logiciels nécessaires au raccordement à Internet d'une entreprise tout en lui garantissant un contrôle d'accès ne remettant pas en cause la pérennité de son système d'information.

Ce TP vous permettra, dans un premier temps, de découvrir la technologie IP ADSL et son paramétrage associé permettant le raccordement du site à l'Internet. Dans un second temps, vous découvrirez les mécanismes et les règles de sécurité à mettre en œuvre sur un réseau local d'entreprise pour le protéger des agressions extérieures donc de garantir aux utilisateurs un accès aux informations et ressources disponibles sur Internet mais aussi lui permettant d'être visible depuis l'Internet sans risques.

3.2 Architecture physique du réseau à mettre en œuvre



3.3 Accès Internet

Interface EXTERNE :

Pour la partie EXTERNE du firewall, elle fera partie du réseau *62.244.110.64/29*, la station PC2 possédera l'adresse IP *62.244.110.66* pour nos tests, le commutateur aura l'adresse *62.244.110.65* et la partie Ethernet 0 du routeur CISCO 837 l'adresse IP *62.244.110.70*. La partie EXTERNE du firewall aura pour adresse IP : *62.244.110.67*.

Interface OPTIONAL (ou DMZ) :

L'interface OPTIONAL possédera l'adresse de réseau *62.244.110.72/29* et le serveur WWW, FTP, SMTP aura pour adresse IP *62.244.110.74*. La partie OPTIONAL du firewall aura pour adresse IP *62.244.110.73*.

Interface TRUSTED (ou MZ) :

Pour l'interface TRUSTED, nous pouvons choisir un plan d'adressage de type privé, dans notre cas nous prendrons un réseau de classe C privé : *192.168.0.0*, et la station PC1 aura pour adresse IP : *192.168.0.2*. La partie TRUSTED du firewall aura pour adresse IP : *192.168.0.1*.

3.4 Paramétrages du routeur d'accès Internet côté réseau LAN

Tout d'abord, avant de commencer à configurer le routeur CISCO 837 et le commutateur C2950, il faut faire une remise en configuration d'usine à l'aide de la commande suivante :

Pour le commutateur :

Effacement de la configuration, du vlan et redémarrage :

- *erase startup-config*
- *Dir flash :*
- *delete flash : vlan.dat*
- *reload*

Pour le routeur :

Effacement de la configuration, et redémarrage :

- *erase startup-config*
- *reload*

3.4.1 Sur le routeur CISCO 837

Pour la configuration du routeur CISCO 837, il faut, à l'aide du logiciel HyperTerminal et via le port série (9600, 8, N, 1) taper les commandes suivantes :

conf terminal
enable secret rle
line vty 0
password vt
exit
interface ethernet 0
ip address 62.244.110.77 255.255.255.248
no shutdown

3.4.2 Sur le commutateur C2950

Pour la configuration du commutateur C2950, il faut taper les commandes suivantes :

conf terminal
enable secret rle
line vty 0
password vt
exit
interface vlan 1
ip address 62.244.110.73 255.255.255.248
no shutdown

3.4.3 Sur la station de travail

Sur la station PC2, dans ‘Connexions réseaux’ on change l’adresse IP de la station en mettant l’adresse IP *62.24.110.78* pour effectuer nos tests lors du TP.

3.5 Validation fonctionnelle sur le réseau local

Au niveau physique :

Une fois les équipements d’interconnexion branchés et configurés, les voyants de mise sous tension et de communication sur le routeur et le commutateur sont bien allumés et verts signe de bonne communication.

Au niveau trame (Ethernet) :

Tout d’abord nous pouvons vérifier l’interface de management du vlan 1 par la commande *show running-config* :

```
interface Vlan1
 ip address 62.244.110.65 255.255.255.0
 no ip route-cache
!
```

On peut également faire un *show ip interface brief* :

```
Commut4#show ip int brief
Interface                  IP-Address      OK? Method Status
ocol
Vlan1                      62.244.110.65   YES manual up
```

Au niveau paquets (IP) :

Ensuite nous avons vérifié si la connexion entre les différents éléments était correcte grâce à la commande *ping* :

```
D:\Documents and Settings\etudiant>ping 62.244.110.70

Envoi d'une requête 'ping' sur 62.244.110.70 avec 32 octets de données :

Délai d'attente de la demande dépassé.
Réponse de 62.244.110.70 : octets=32 temps=1 ms TTL=255
Réponse de 62.244.110.70 : octets=32 temps=1 ms TTL=255
Réponse de 62.244.110.70 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 62.244.110.70:
    Paquets : envoyés = 4, reçus = 3, perdus = 1 (perte 25%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Ensuite nous avons effectué un *ping* vers l'adresse *62.244.110.65* avec succès.

3.6 Paramétrage du routeur d'accès Internet côté réseau WAN

Pour configurer le routeur CISCO 837, il faut se connecter en INBAND via le logiciel telnet puis il faut rentrer en mode ENABLE puis ensuite rentrer les commandes suivantes :

conf t
interface atm 0
dsl operating-mode auto
interface atm 0.1 point to point
pvc 8/35
pppoe-client dial-pool-number1

Puis :

interface dialer 0
ip address negotiated
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication pap chap callin
ppp chap hostname iutangers.crt@ip10.bluegix
ppp chap password 0 jplcv2007
ppp pap sen iutangers.crt@ip10.bluegix password 0 jplcv2007

exit

ip route 0.0.0.0 0.0.0.0 dialer 0
ip route 62.244.110.72 255.255.255.248 0.0.0.0

dialer-lis 1 proto ip permit

Une fois avoir configuré le CISCO 837, la connexion ne fonctionnait toujours, mais nous avions oublié de faire un *no shutdown* et également un *ip routing* pour pouvoir rentrer les routes.

3.7 Validation fonctionnelle sur le réseau WAN

Au niveau physique :

Le voyant CD ADSL est allumé, et les voyants RD et TD ADSL clignotent lors que l'on effectue un ping vers l'extérieur (vers le DNS par exemple).

Au niveau cellule (ATM) :

Voici un imprime écran des interfaces (il a fallut ensuite faire un *no shutdown* sur l'interface ATM0 car on voit bien qu'elle est shutdown) :

```
interface ATM0
 no ip address
 no ip route-cache
 shutdown
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.1 point-to-point
 no ip route-cache
 no snmp trap link-status
 pvc 8/35
  pppoe-client dial-pool-number 1
 !
```

Au niveau paquets (IP):

Nous avons effectués un ping vers le DNS pour vérifier si la connexion vers l'extérieur fonctionnait et effectivement nous pouvions pinger le serveur DNS.

4. Mise en œuvre du firewall de l'entreprise

4.1 Objectifs de la manipulation

Le firewall de la marque Watchguard de type Firebox II est un équipement permettant de sécuriser le réseau informatique de l'entreprise.

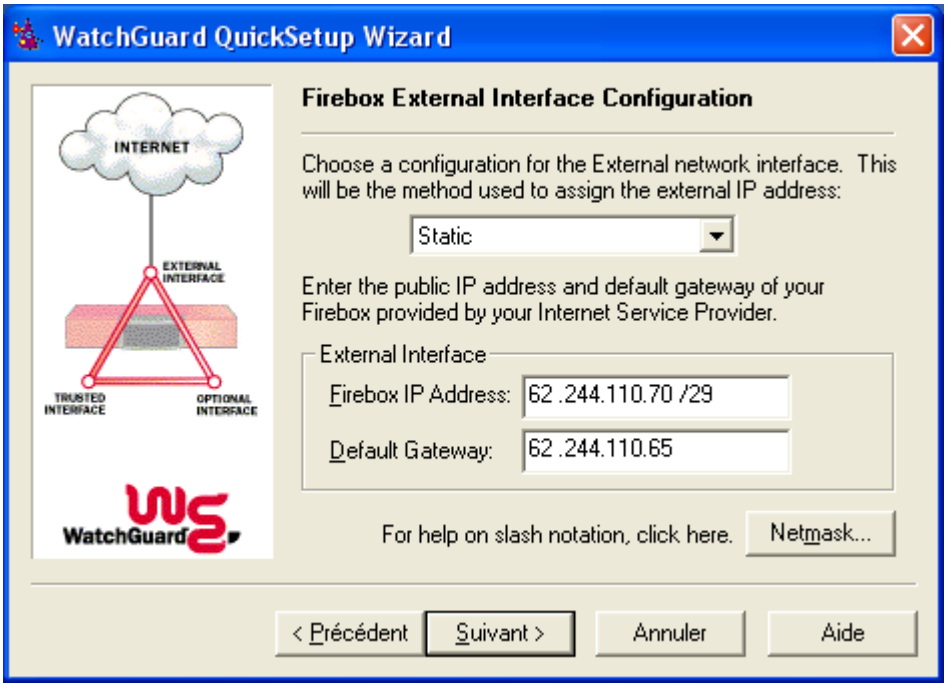
4.2 Spécifications à respecter pour la configuration du firewall

Le firewall sera configuré en more routeur, il sera la passerelle par défaut pour les équipements raccordés à ses interfaces. Le but du firewall est d'autorisé la MZ à communiquer avec l'Internet mais que l'Internet ne voit pas la MZ, que l'Internet puisse juste avoir accès à la DMZ pour pouvoir accès au serveur WWW, FTP et SMTP.

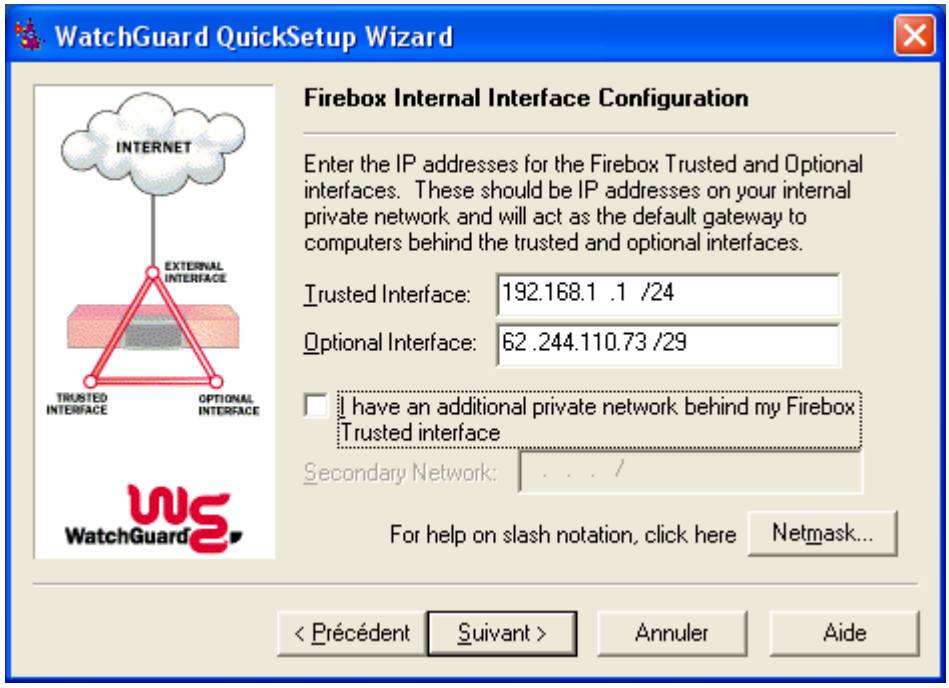
4.3 Eléments d'information sur le firewall

Pour la configuration du firewall, il faut lancer le logiciel 'Quick Setup Wizard' et ensuite suivre les indications. Mettre l'adresse du pc qui le configure, puis ensuite configurer l'adresse IP du lien Externe, Trusted et Optional :

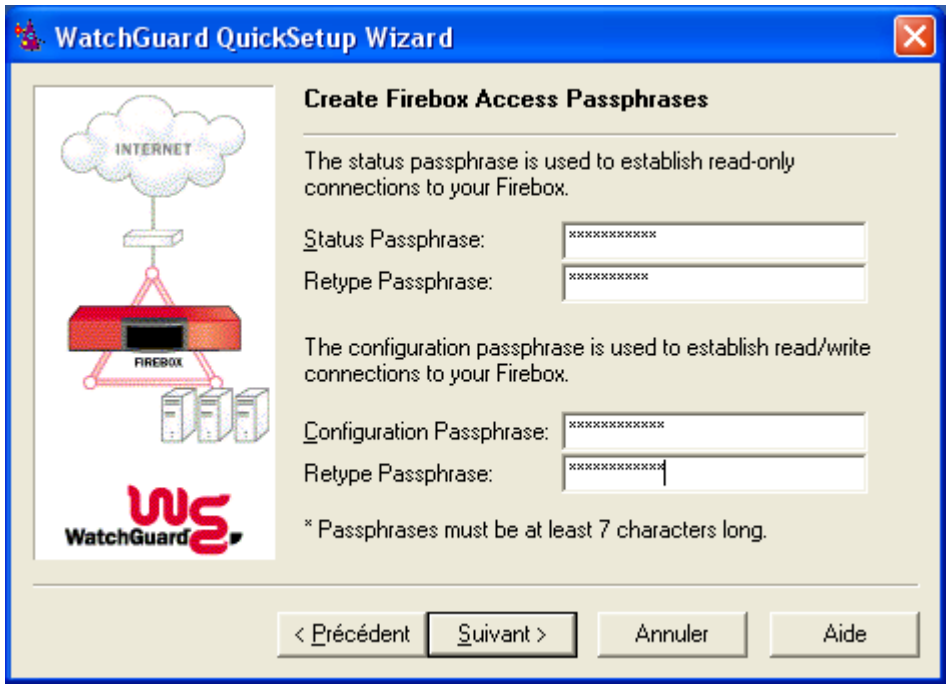
Configuration du lien Externe :



Configuration du lien Trusted et Optional :



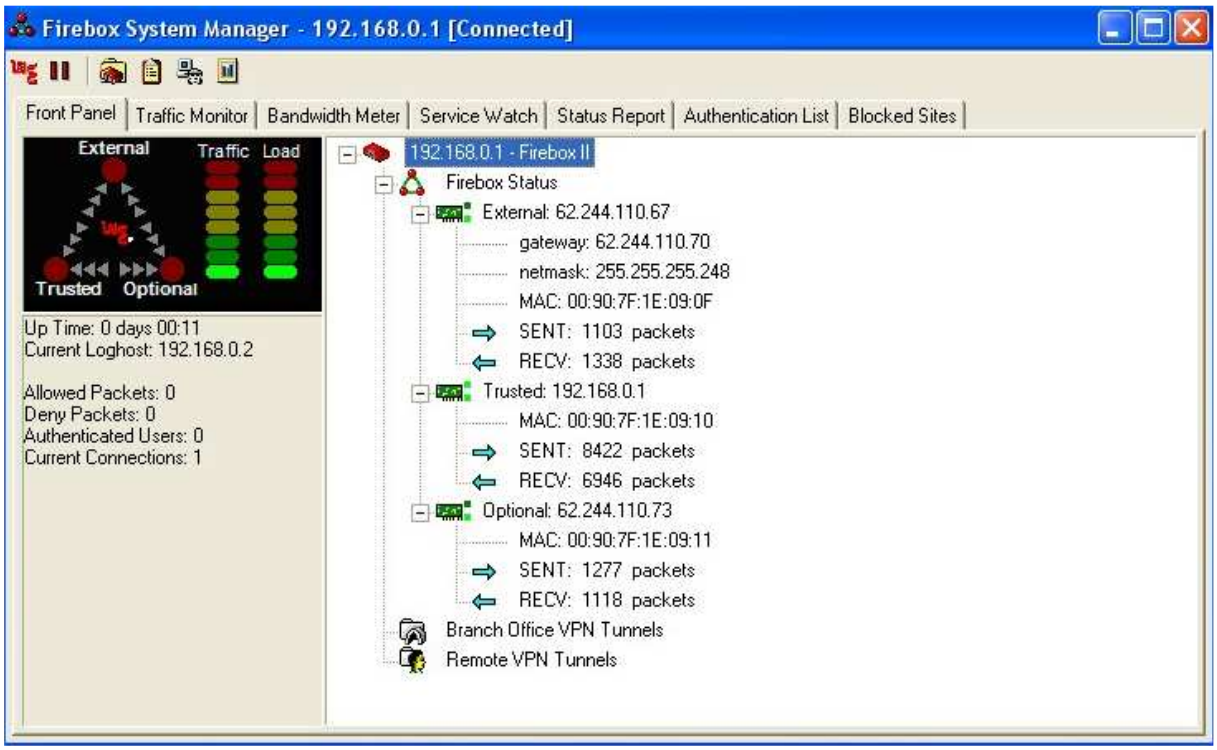
Configuration des mots de passe pour ensuite avoir accès au Firewall :



4.4 Mise en œuvre de la solution

Pour mettre en œuvre la solution il a fallut se servir de l'interface graphique du firewall Firebox II.

Tout d'abord, on peut voir quelque information à l'aide du front panel :

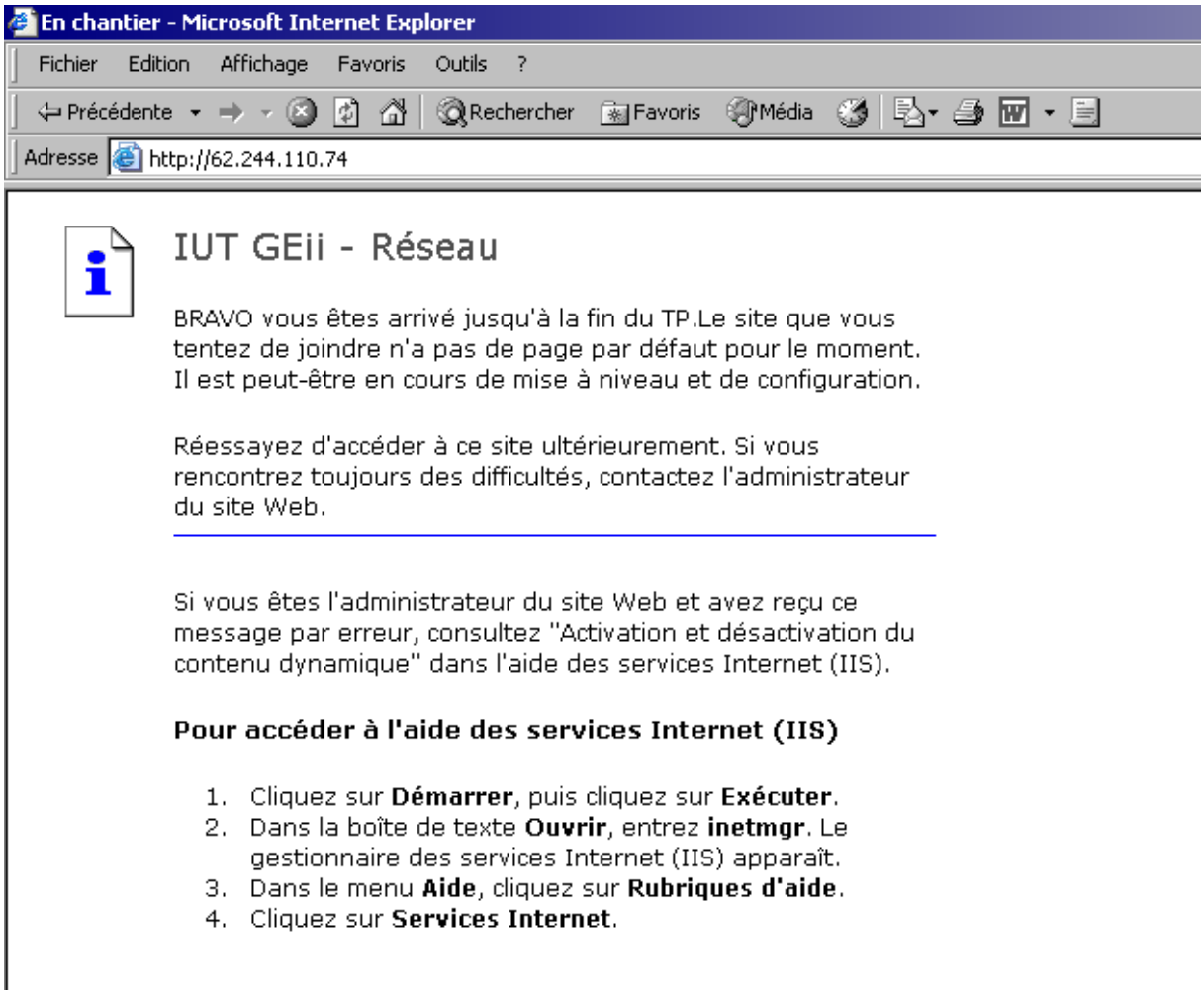


Et pour la configuration, il a fallut utiliser cette interface graphique :

Il a fallut faire en sorte que seule la DMZ soit accessible de l'Internet (grâce à son IP public) mais que la MZ soit protéger de l'Internet, mais qu'elle puisse quand même avoir accès à la DMZ et à l'Internet.

5. Accès au serveur WEB depuis le réseau de l'Université

Pour clore le TP, à partir du poste de l'enseignant voici ce que l'on trouve à l'adresse du serveur WEB sous Windows :



6. Conclusion

Ce TP nous a permis de mettre en place pour la première fois un firewall autre que les firewall logiciel que l'on peut trouver, de plus avec son interface graphique simple cela nous a permis de plus penser aux notions importantes comme le fait que la MZ soit bien protéger de l'Internet par exemple. Un firewall est un matériel indispensable dans un réseau d'entreprise et donc nous pensons que c'est important d'avoir des notions sur les firewalls.