

Configuration d'un firewall pour sécuriser un serveur WEB

Contexte : Dans le cadre de la mise en place d'un serveur intranet, il est demandé de sécuriser son accès et de le personnaliser en fonction de la provenance de l'utilisateur.

Objectifs : Sécuriser l'accès au serveur web par un firewall pour deux réseaux locaux différents, le réseau du service informatique et le réseau des utilisateurs.

Description de l'activité réalisée

Situation initiale : Le serveur web n'est pas sécurisé, les accès vers celui-ci ne peuvent être ni restreint ni contrôlés.

Situation finale : Après la réalisation de l'activité, le serveur web est totalement sécurisé. Les différents réseaux de l'entreprise ont des accès personnalisés, un fichier historique (log) permet une surveillance active de la sécurité du serveur web.

Outils utilisés : Nous avons utilisé une distribution linux sur laquelle nous avons installé un firewall (iptables) et son manager (fwbuilder).

Déroulement de l'activité :

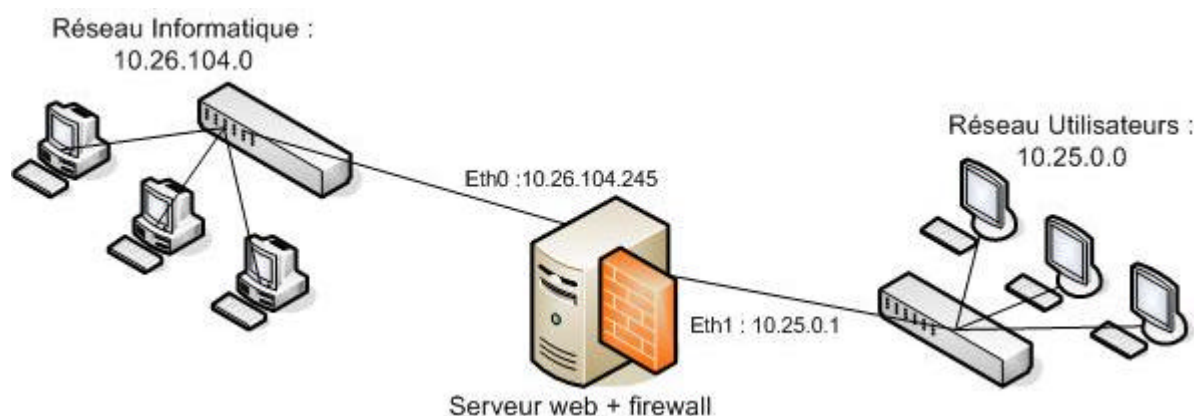
Le réseau de l'entreprise se présente donc sous la forme de 2 réseaux distincts :

?? Le réseau informatique : 10.26.104.0 / 255.255.255.0

?? Le réseau utilisateurs : 10.25.0.0 / 255.255.255.0

Le serveur web possède donc 2 interfaces réseaux connectées chacune sur un réseau différent. L'interface eth0 a pour adresse ip : 10.26.104.245 et est connectée sur le réseau du service informatique.

L'interface eth1 a pour adresse ip : 10.25.0.1 et est connectée sur le réseau utilisateurs.



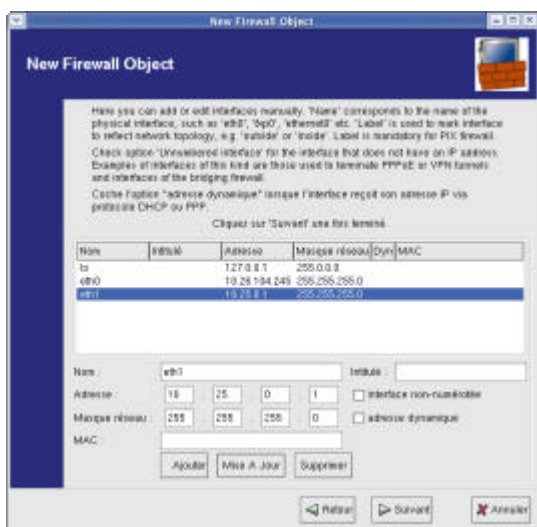
Le réseau des utilisateurs ne doit avoir accès au serveur web uniquement via le port 80.
Le réseau du service informatique lui doit avoir un accès sur le port 80 bien sur mais aussi sur le ftp,
sur des sessions SSH et par VNC.

1) Installation du firewall

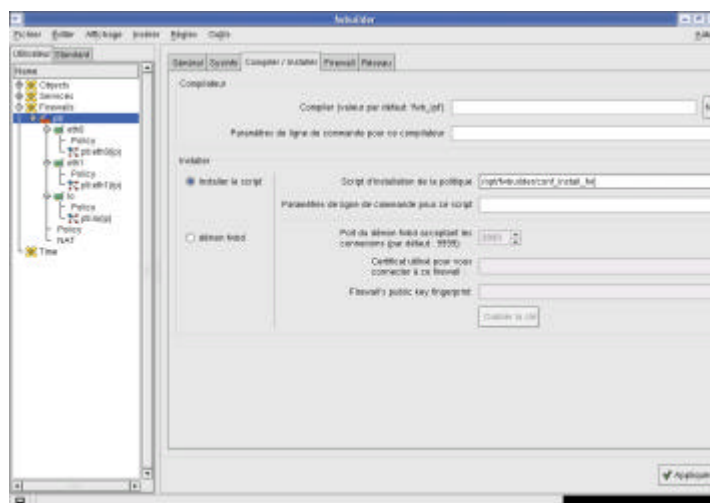
L'installation du firewall se fait via des fichiers sources téléchargés sur le site www.fwbuilder.org

2) Configuration du firewall

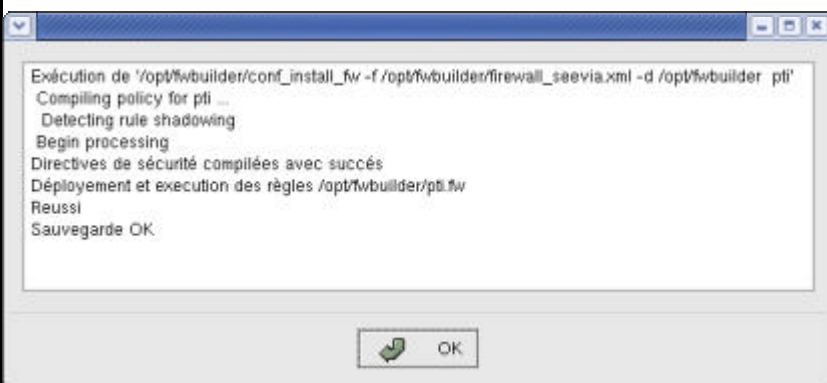
Commençons par créer notre objet firewall en lui paramétrant les différentes interfaces dont il dispose.



Notre objet firewall est maintenant créé nous allons maintenant le configurer pour que fwbuilder puisse « manager » iptables, pour cela nous lui indiquons le chemin vers le script d'installation.

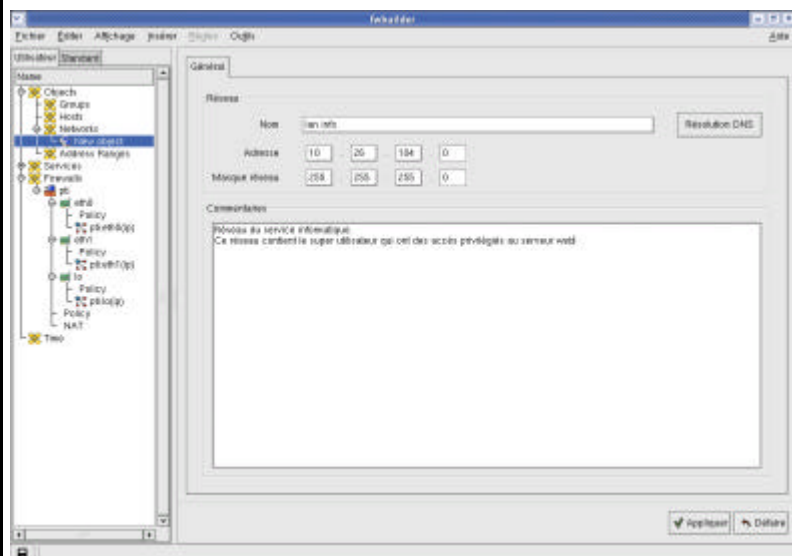


Nous allons maintenant faire une compilation de cette configuration, fwbuilder va donc créer un fichier .xml résumant la configuration qui jusqu'ici a été choisie.

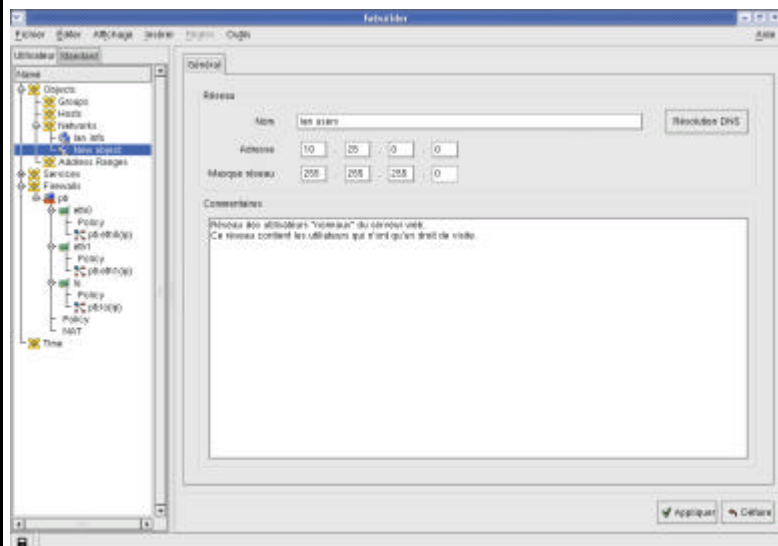


Nous allons ensuite créer les deux objets représentant les deux réseaux.

- o Lan info pour le réseau du service informatique.



- o Lan users pour le réseau des utilisateurs.

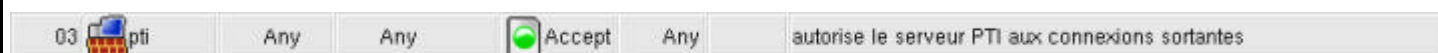


3) Création de la politique de sécurité

Nous allons maintenant créer les règles sur le firewall nécessaire à la sécurisation du serveur web. Notre politique de sécurité est de refuser tout ce qui n'est pas accepté, nous commençons donc par créer une règle refusant tout.



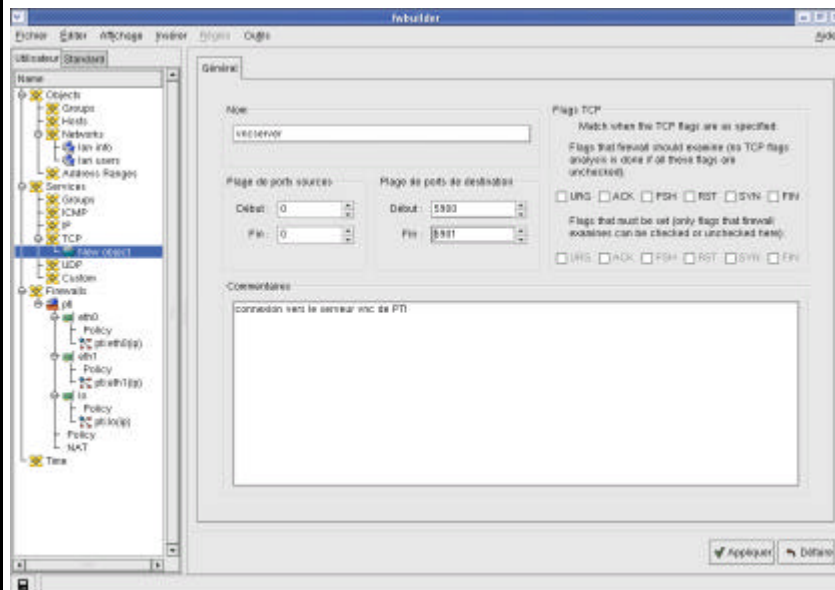
Puis nous allons autoriser le serveur web à se connecter en sortie sans restriction.



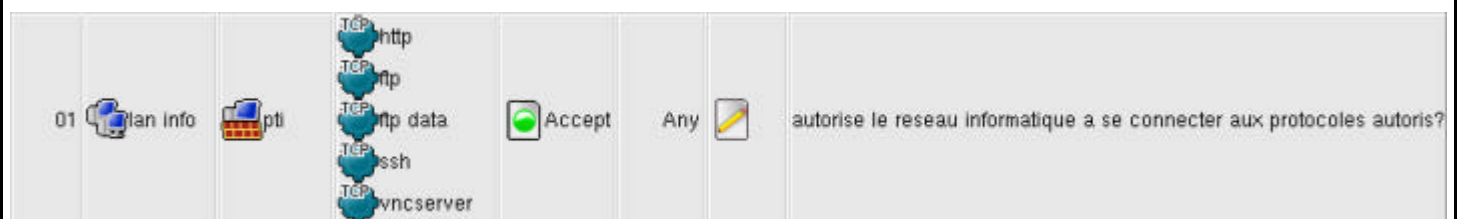
Procédons à l'autorisation pour le réseau des utilisateurs à se connecter au serveur web sur le port 80.



Créons maintenant la règle pour autoriser le réseau du service informatique à se connecter aux différents protocoles autorisés.
Avant cela il nous faudra créer un objet nommé vncserver pour autoriser les accès vers le serveur VNC par le réseau du service informatique.



La règle donc autorise le réseau informatique à se connecter sur le port 80, le port 21, le port 20, le port 22 et les ports 5900 et 5901



Une fois les règles mises en place, il nous faut compiler les modifications et les implémenter sur « iptables ».

Toutefois il faudra bien s'assurer de mettre en place un chmod 777 sur le fichier de configuration du firewall pour être sûr que les règles soient bien installées sur « iptables ».

4) Vérification de la sécurité

Nous pouvons donc vérifier si les règles sont en place protège bien le serveur web.

Nous demandons donc au responsable du service informatique de se connecter sur le serveur web via le http, le ssh, le ftp et vnc.

Tous les protocoles sont ok

Par exemple le protocole ftp :

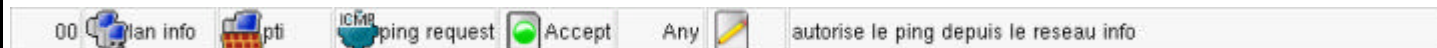
```
C:\>ftp 10.26.104.245
Connected to 10.26.104.245.
220 (vsFTPd 1.1.3)
User (10.26.104.245:(none)): sys-ops
331 Please specify the password.
Password:
230 Login successful. Have fun.
ftp>
ftp>
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp>bye
```

Alors que les utilisateurs eux ne sont autorisés qu'à l'accès au serveur http et se voit refuser toute autre connexion.

5) Règle de simplification d'administration du serveur

Pour simplifier l'administration du serveur par le service informatique, nous allons leur autoriser le ping vers le serveur pour être sûr qu'il soit en mesure de procéder à des diagnostics rapides en cas de panne.

Nous ajoutons donc une règle supplémentaire.



Effectuons un test de ping depuis le réseau du service informatique.

```
C:\>ping 10.26.104.245
```

```
Pinging 10.26.104.245 with 32 bytes of data:
```

```
Reply from 10.26.104.245: bytes=32 time<10ms TTL=64
```

```
Reply from 10.26.104.245: bytes=32 time<10ms TTL=64
```

```
Reply from 10.26.104.245: bytes=32 time<10ms TTL=64
```

```
Reply from 10.26.104.245: bytes=32 time<10ms TTL=64
```

```
Ping statistics for 10.26.104.245:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Analyse des résultats obtenus

Objectif atteint : Le site web est totalement sécurisé grâce à la mise en place du firewall et de la politique de sécurité. Les différents utilisateurs des réseaux se voient attribuer des accès vraiment personnalisés.