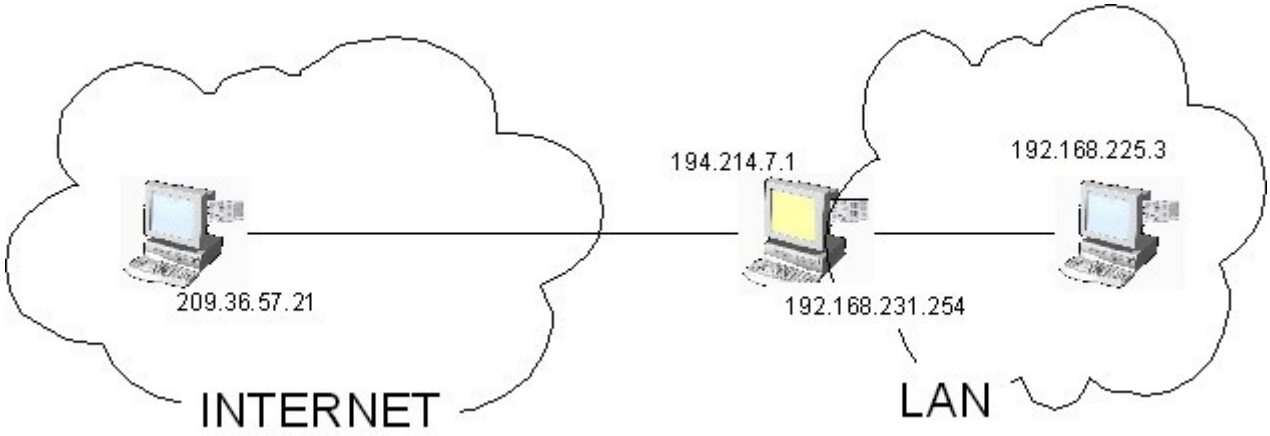
PAT et NAT : Des mécanismes pour accéder aux ressources du LAN

Le schéma suivant illustre le cas de nombreux réseaux :

- la connexion à internet se fait via un routeur mandataire (proxy router)
- les machines dans le LAN ont des adresses privées, y compris les serveurs.



Dans ce cas :

- seule la machine 194.214.7.1 peut répondre aux requêtes venant d'internet.
- cette machine doit avoir des règles de **forwarding** pour que ces requêtes soient redirigées vers 192.168.225.3

Principe de fonctionnement :

Rappel
un message internet comporte deux informations fondamentale : l'adresse IP désigne un ordinateur unique sur internet; le n° de port TCP désigne le logiciel destinataire de ce message. Exemple : http://www.google.fr : 4200

La **clé** de ce mécanisme, c'est **le n° de port TCP** de destination du message.

Voici par exemple des règles qui pourraient être utilisées sur le routeur 194.214.7.1, avec leur interprétation :

Port destinataire	Machine destinataire **avant** forwarding	Machine destinataire **après** forwarding	Interprétation
80	194.214.7.1	192.168.225.3	Le serveur web est sur 192.168.225.3
22	194.214.7.1	pas de forwarding	194.214.7.1 a son propre serveur ssh
2222	194.214.7.1	192.168.225.3	Le serveur ssh de 192.168.225.3 répond sur le port 2222
25	194.214.7.1	192.168.225.3	Le serveur smtp est sur 192.168.225.3
110	194.214.7.1	192.168.225.3	Le serveur pop est sur 192.168.225.3

Ici, nous n'avons modifié que l'adresse de destination du message (NAT = Network Adress Translation); Ceci nous a obligé a configurer le serveur ssh de 192.168.225.3 pour répondre sur le port 2222.

On aurait pu aussi modifier le port de destination du message (PAT = Port Adress Translation).

Ce qui aurait donné :

Port destinataire **avant** forwarding	Machine destinataire **avant** forwarding	Machine destinataire **après** forwarding	Port destinataire **après** forwarding	Interprétation
80	194.214.7.1	192.168.225.3	80	Le serveur web est sur 192.168.225.3
22	194.214.7.1	pas de forwarding	22	194.214.7.1 a son propre serveur ssh
2222	194.214.7.1	192.168.225.3	22	Le serveur ssh de 192.168.225.3 sur le port 22
25	194.214.7.1	192.168.225.3	25	Le serveur smtp est sur 192.168.225.3
110	194.214.7.1	192.168.225.3	110	Le serveur pop est sur 192.168.225.3

Le serveur ssh de 192.168.225.3 répond de façon standard sur le port 22; mais pour y accéder de l'extérieur, on doit utiliser le port 2222; c'est ce qui permet de le distinguer du ssh de 194.214.7.1.

C'est le routeur-proxy qui modifie la requête en remplaçant 2222 par 22 avant de la transmettre à 192.168.225.3.

Dans ce cas, on a à la fois du NAT et du PAT.

Cas du routeur D-LINK 624

Commentez les deux règles déjà crées sur ce routeur ADSL D-LINK dans la rubrique « virtual server » :

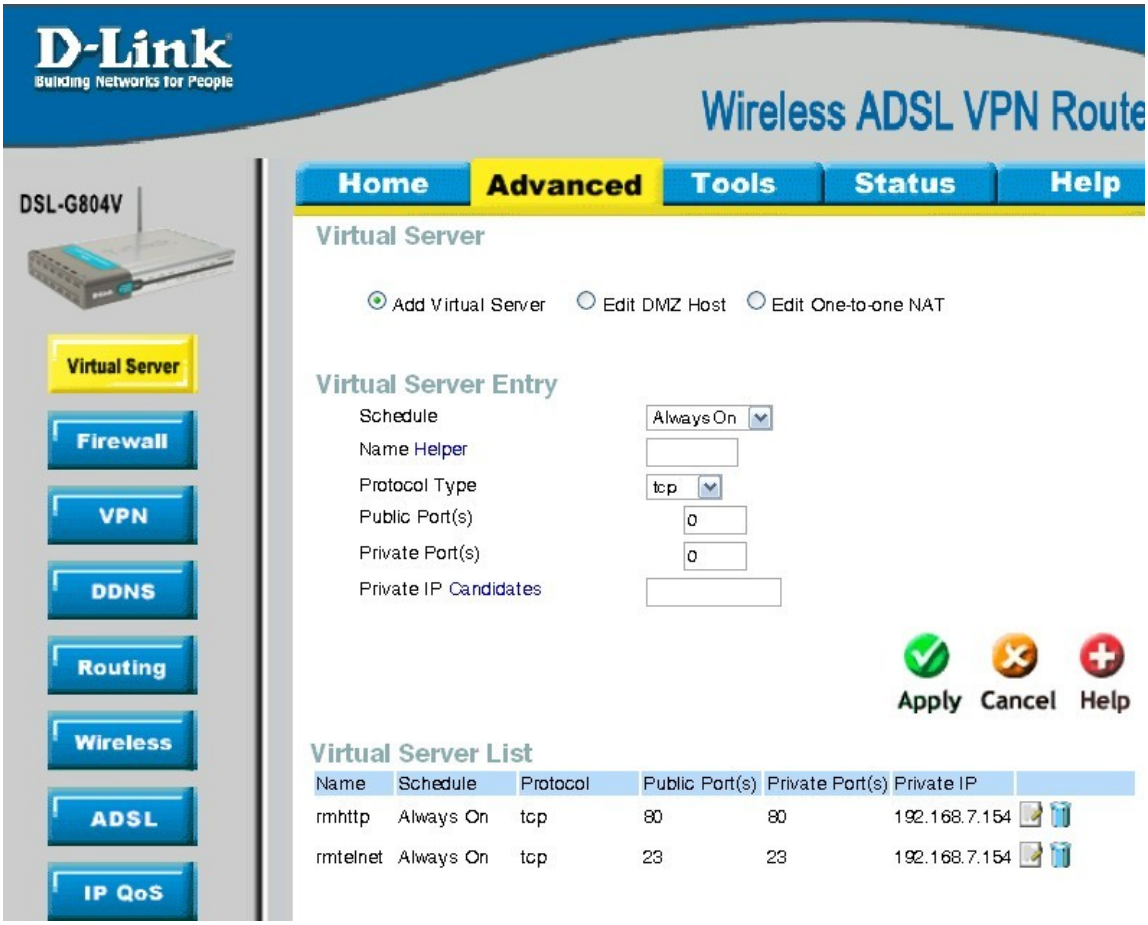
_____

_____

_____

Exercice : Renseigner les paramètres pour créer une règle afin de rendre le serveur openSSH de la machine 192.168.7.250 disponible depuis internet avec le port 2222. (openSSH est configuré avec le port ssh standard)

Schedule	
Name helper	
Protocol type	
Public port	
Private port	
Private IP	



Cas d'iptables (EOLE AMON)

iptables désigne la couche de filtrage et de routage de GNU/Linux;

Il se configure à l'aide d'un script de configuration qui est exécuté à chaque démarrage du serveur.

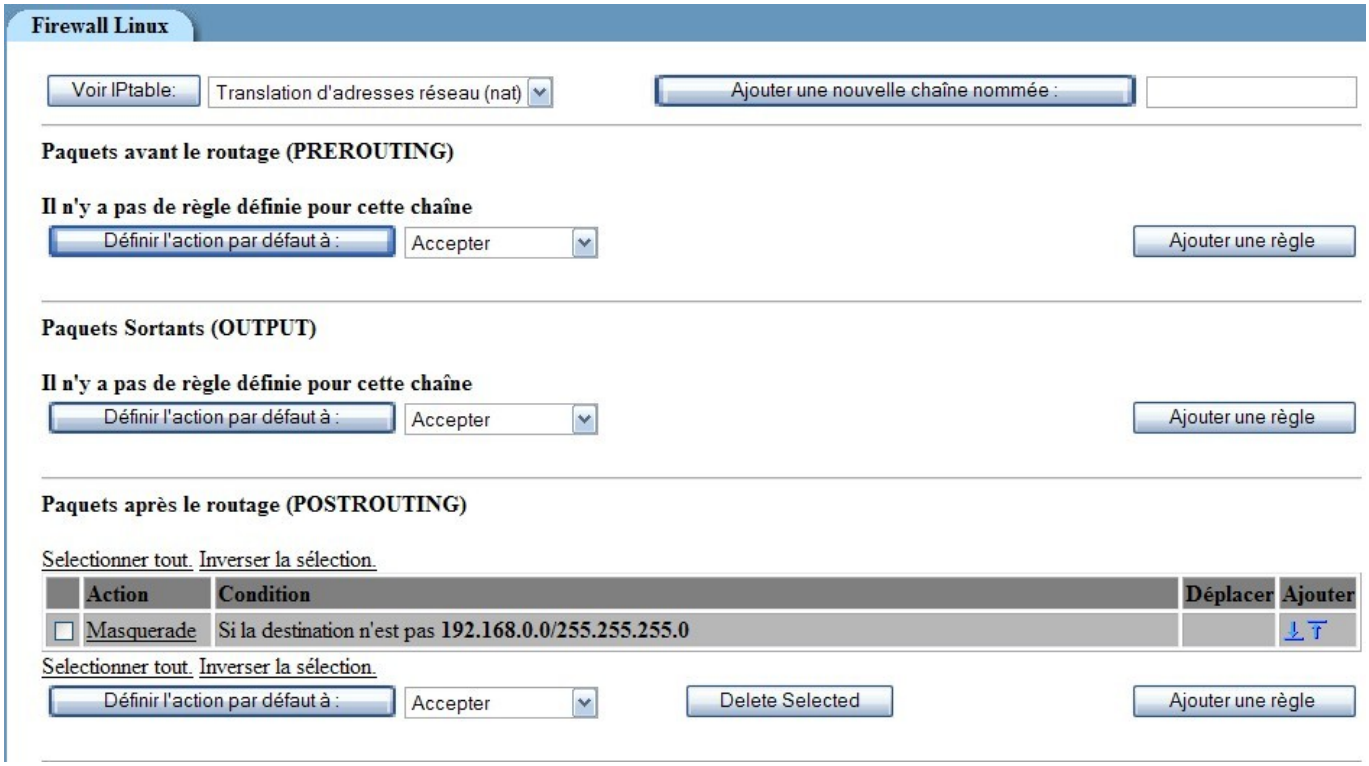
Webmin permet de créer/modifier ce script d'une façon plus « conviviale »

La partie qui nous intéresse est la partie NAT :

Dans cette rubrique, on peut créer trois type de règle :

- PREROUTING :
- OUTPUT :
- POSTROUTING :

En expliquant le rôle de chacun de ces type de règles, désigner celle qui nous intéresse :



Voyez ci-dessous le formulaire qui permet de créer une règle PREROUTING.

Considérez les paramètres entrés ici (surlignés); quel va être l'effet attendu de cette règle ?