

0.1 Partage de connexion : passerelle Linux

Dans ce document je vais détailler la configuration d'un serveur Linux partageant une connexion sans firewall. Pour ceux qui souhaitent également monter un firewall, le détail de la configuration d'Iptables/Netfilter est vu ICI¹. Ceci étant précisé, lorsque vous disposez d'une connexion unique à Internet à partager à plusieurs, vous avez globalement le choix entre 2 stratégies : un proxy ou un nat : Network Address Translation. Un proxy est un mandataire, lorsque votre passerelle fait proxy, cela signifie que les clients ne se connectent pas directement à Internet, mais demande au proxy de télécharger pour eux les pages dont ils ont besoin. Un proxy quelqu'il soit ne couvre qu'une gamme limitée de protocole, généralement http et ftp. Un nat est plus transparent et c'est lui que nous étudions.

0.1.1 1. Les pré-requis :

- Sur le serveur vous devez avoir installé Iptables.
- Vous devez connaître les DNS 1 et 2 de votre FAI
- Sur le serveur vous devez avoir les modules suivants (dans /lib/modules/votre_noyau/kernel/net/ipv4/netfilter/):

```
ip_conntrack_ftp
ip_conntrack_irc
ip_conntrack
iptables_nat
iptables_filter
```

Si vous utilisez le noyau natif d'une des distributions suivantes : Mandriva, Redhat, Debian et Slackware, ce qu'il faut est déjà présent, soit en module (option M) soit en dur (Option Y). Pour les autres, qui n'ont pas ces modules, une recompilation² du noyau s'impose. Dans tous les cas, assurez-vous que ces modules seront chargés à chaque amorce de votre passerelle, en utilisant l'outil de votre distribution. Autre méthode, vous pouvez rajouter les lignes suivantes à votre /etc/rc.d/rc.local :

```
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_conntrack_irc
/sbin/modprobe ip_conntrack
/sbin/modprobe iptable_nat
/sbin/modprobe iptable_filter
```

Ne rajoutez que les lignes qui chargent les modules physiquement présent sur votre système.

- Créez un fichier nat.sh sur la passerelle, contenant ceci :

```
#!/bin/sh
echo "[Activation du partage de connexion]"
echo "1" > /proc/sys/net/ipv4/ip_forward
```

- rendez nat.sh exécutable par :

```
chmod 755 nat.sh
```

¹<http://www.trustonme.net/didactels/112.html>

²<http://www.trustonme.net/didactels/194.html>

0.1.2 2. Translation d'adresse source ou masquerading :

Le masquerading est une translation d'adresse source, c'est à dire qu'il remplace les adresses source des paquets d'un réseau local, par l'IP de la passerelle. Il conserve cependant des traces des transactions pour acheminer vers chacun, le paquet qui lui est destiné. Ainsi, toutes vos machines apparaissent sur Internet comme une seule et même machine. Grâce au masquerading, tous les logiciels clients (mozilla, kmail, pan ...), installés sur les ordinateurs de votre réseau, peuvent accéder à internet de manière transparente. Pour activer, le masquerading, rajoutez la ligne suivante à votre nat.sh :

```
echo "[Mise en place du masquerading]"
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o ppp0
-j MASQUERADE
```

Ceci suppose que vous ayez un réseau en 192.168.0.x, adaptez à votre configuration.

0.1.3 3. Translation d'adresse de destination ou portforwarding :

Le portforwarding c'est l'opération inverse du masquerading. Il remplace les adresses destination des paquets arrivant vers la passerelle, par les adresses réelles des serveurs sur le réseau local. C'est cette propriété qui vous permet d'héberger un serveur web apache, par exemple, sur la machine d'adresse 192.168.0.7, alors que la machine physiquement connectée à internet a pour adresse locale 192.168.0.1 (votre passerelle). Les clients Internet d'apache, tapent l'adresse internet (ou le nom de domaine) de la passerelle et accède à votre serveur apache, comme si ce dernier était physiquement hébergé sur la passerelle. Pour activer le portforwarding, il faut faire une étude par cas, mettons que je veuille forwarder mon serveur apache (port 80), situé sur 192.168.0.7, je rajoute à nat.sh :

```
echo "[Seveur Apache(80) sur 192.168.0.7]"
iptables -A FORWARD -i ppp0 -p tcp -dport 80 -j ACCEPT
iptables -t nat -A PREROUTING -j DNAT -i ppp0 -p TCP -dport
80 -to-destination 192.168.0.7
```

Adaptez à votre réseau et à vos serveurs. Pour tester, donnez l'IP internet de la passerelle à un ami et vérifiez qu'il accède au serveur. Suivez, la même logique pour **ssh(22)**, **smtp(25)**, **https(443)**, **DNS(53)**, **irc(6667)** ou plus généralement **montruc(1425778)**. Vous pouvez en mettre autant que nécessaire.

0.1.4 4. Configuration des clients :

0.1.5 4.1 Clients Linux :

Je suppose dans la suite que votre réseau sur chaque client Linux est configuré. Notamment, que vous puissiez pinguer votre passerelle depuis le client Linux. Si ce n'est pas votre cas, reportez-vous à ceci³ Quand vous êtes près, tapez la ligne suivante, en root dans un terminal: `/sbin/route add -net default gw 192.168.0.1 netmask 0.0.0.0 metric 1` remplacez 192.168.0.1 par l'IP de votre passerelle. Ensuite, lancez le logiciel de configuration du réseau de votre distribution et indiquez lui comme passerelle, l'adresse locale de votre passerelle (192.168.0.1), si ce n'est pas déjà fait. Finissez en rajoutant ce qui suit à votre `/etc/resolv.conf` :

³<http://www.truostonme.net/didactels/101.html>

```
nameserver DNS_1_de_votre_FAI
nameserver DNS_2_de_votre_FAI
```

Pour **wanadoo**, les DNS 1 et 2 sont : 80.10.246.2 et 80.10.246.129 Pour **Free**, les DNS 1 et 2 sont : 212.27.32.176 et 212.27.32.177

0.1.6 4.2 Clients Windows :

je suppose dans la suite que votre réseau est fonctionnel sous Windows. Notamment que depuis windows, vous puissiez pinguer la passerelle. Si votre réseau, sous windows, n'est pas fonctionnel, reportez-vous à l'un des nombreux sites de vulgarisation sur cet OS. La configuration est en tout point similaire à celle que vous auriez eue, à faire avec un nat géré par sygate, par exemple. Concrètement, rendez-vous dans le "voisinage réseau" (ou "connections réseaux et accès à distance"). Là choisissez votre carte réseau et allez dans "propriétés". Double-cliquez sur "Protocole Internet (TCP/IP)". Là comme "passerelle par défaut" mettez l'IP de la passerelle. Comme "DNS préféré" mettez le DNS 1 de votre FAI, comme DNS auxiliaire le DNS 2 de votre FAI. Selon votre version de Windows, il se peut que vous ayez à valider par "ajouté" à chaque onglet. Une fois satisfait validez et c'est bon. Pour **wanadoo**, les DNS 1 et 2 sont : 80.10.246.2 et 80.10.246.129 Pour **Free**, les DNS 1 et 2 sont : 212.27.32.176 et 212.27.32.177.

0.1.7 5. Lancement du partage :

De retour sur la passerelle, copiez le fichier nat.sh dans /usr/bin/, vous pouvez désormais activer le partage de connexion en tapant :

```
/usr/bin/nat.sh
```

Si vous souhaitez que le partage soit actif dès le démarrage de la machine, rajoutez ceci à /etc/rc.d/rc.local :

```
/usr/bin/nat.sh
```