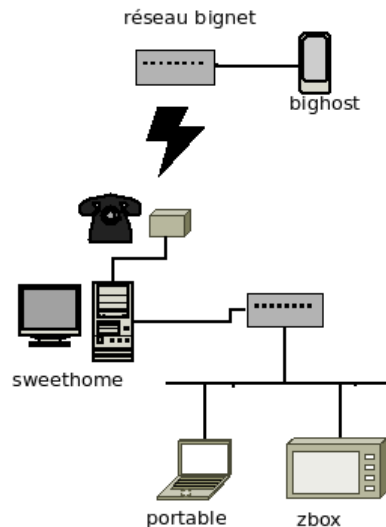


## Filtrage

Vous avez pris un abonnement chez un FAI<sup>1</sup> (ici **bignet.com**). Vous cherchez tout d'abord à protéger le poste de travail familial "sweethome" des attaques éventuelles.

La famille s'équipant, apparaît ensuite le besoin de *partager la connexion Internet* (le FAI ne fournit qu'une ligne avec une adresse IP) avec divers équipements (ici un portable et une console de jeu **zbox**), que l'on raccorde par un switch ; le poste de travail - muni d'une seconde carte réseau - agissant comme routeur.

Et ensuite, vous voulez que le jeu en réseau qui tourne sur le serveur web de la Zbox soit accessible de l'extérieur...



## 1 Préparation

Dans `/net/Bibliotheque/ASR4-Reseaux/FILTRAGE/` se trouvent

- un script `installer-machines`, lancez-le pour copier les 4 machines virtuelles de l'exercice dans votre répertoire `/.cows`,
- un script `reseau-maison` simulant le réseau, copiez-le dans votre espace de travail.

## 2 Exploration

Au départ, le script de simulation de réseau `reseau-maison` ne lance que les deux machines `sweethome` et `bighost`.

1. Connectez-vous sur les deux machines. Faites un plan du réseau avec les adresses IP utilisées. Donnez la table de routage de chacune des machines et précisez le(s) serveur(s) de noms utilisé(s).
2. Étudiez le domaine DNS géré par `bighost` (n'hésitez pas à regarder les fichiers de configuration!) : son nom, les fichiers où sont stockés les données. Donnez les adresses IP de `www.bignet.com`, `dns.bignet.com`, `poste.bignet.com` et `autre.bignet.com`.

---

1. Fournisseur d'Accès à Internet

3. Étudiez le domaine DNS géré par `sweethome` (n'hésitez pas à regarder les fichiers de configuration!) : son nom, les fichiers où sont stockés les données. Donnez les adresses IP de `sweethome.localdomain`, `dns.localdomain`, `zbox.localdomain` et `portable.localdomain`.
4. Listez les noms associés à une adresse IP de `sweethome`.
5. Sur le poste de travail `sweethome`, le script `/etc/init.d/firewall` contient les règles de filtrage activées à chaque démarrage. C'est ce script qu'il faudra développer pendant cet exercice.
  - Quand est-il lancé exactement ?
  - Pour quelle raison choisit-on ce moment précis ? (les points d'entrée pour répondre à ces questions sont `/etc/inittab` et `/etc/rc*.d`)

### 3 Protection de `sweethome`

1. Déterminez quels services tournent sur `bighost` et `sweethome` (`ssh`, `dns`, `web`...) : utilisez `ps -aux`, `netstat -a`, regardez `/var/log/messages`,...
2. Depuis le poste de travail, tentez un ping vers `bighost.bignet.com`. Regardez le fichier `/etc/init.d/firewall` et expliquez votre échec. Depuis `bighost.bignet.com`, tentez un ping vers le poste de travail. Expliquez votre échec.
3. Ajoutez une règle pour autoriser les pings sortants et entrants. Relancez le script (`/etc/init.d/firewall restart`). Vérifiez, etc.
4. Sur `bighost`, créez un utilisateur `boss`, et donnez-lui un mot de passe :

```
useradd -m boss
passwd boss
```
5. Depuis le poste de travail, tentez une connexion `ssh` sur `bighost` sur le compte de `boss` : `ssh boss@bighost.bignet.com`. Expliquez votre échec.
6. Dans `/etc/init.d/firewall`, ajoutez une ou des règle(s) pour autoriser les connexions `ssh` sortantes. Vérifiez.  
**Indices** : il faut déterminer le protocole transport utilisé par `ssh` (TCP ou UDP), le port destination des datagrammes sortants et le port source des datagrammes entrants.
7. Depuis le poste de travail, tentez des connexions `web` vers `bighost.bignet.com` : `lynx http://bighost.bignet.com` Expliquez votre échec.
8. Dans `/etc/init.d/firewall`, ajoutez une ou des règle(s) pour autoriser les connexions `http` sortantes. Indices : il faut déterminer le protocole transport utilisé par `http`. Il faut aussi déterminer le port destination des datagrammes sortants, et le port source des datagrammes entrants. Vérifiez.
9. Sur `sweethome`, créez un utilisateur à votre nom.
10. Essayez `ssh` vers `poste.bignet.com` depuis `bighost`. Expliquez votre échec.
11. Dans `/etc/init.d/firewall`, ajoutez une ou des règle(s) pour autoriser les connexions `ssh` entrantes. Vérifiez.  
**Indice** : Il faut aussi déterminer le port source des datagrammes sortants, et le port destination des datagrammes entrants.
12. Expliquez la commande `iptables` suivante : `iptables -A INPUT -i eth1 -j ACCEPT`

## 4 Extension du réseau, SNAT

1. Arrêtez proprement (`halt`) les machines virtuelles. Décommentez les deux lignes du script `reseau-maison` qui concernent le `portable` et la `zbox`. Relancez.  
Pour ces deux machines, déterminez leur adresses IP, les routes connues et le serveur DNS utilisé.
2. Depuis le portable, tapez la commande `host bighost.bignet.com`. Que fait cette commande ?  
À quel serveur sont transmises les requêtes DNS de `portable` ? Dans quel fichier, cette information est-elle enregistrée ?  
`sweethome` connaît-il l'adresse IP associée à `bighost.bignet.com` ? Quelles lignes du fichier de configuration `/etc/bind/named.conf` de `sweethome` explique le résultat de la commande `host bighost.bignet.com` ? (pour en être absolument sûr, commentez les 3 lignes, relancez le serveur DNS de `sweethome` et réessayez).
3. Depuis le portable, effectuez des `pings` vers `bighost`, avec son nom, son adresse, etc.  
Lors d'un `ping`, une requête ICMP est envoyée au poste distant, qui doit répondre en envoyant un paquet ICMP à l'émetteur du `ping`. Étudiez les chemins connus par `bighost`, `sweethome`, et `portable` (commande `route`). La requête ICMP est-elle arrivée à `bighost` ? Expliquez.  
La réponse ICMP envoyée par `bighost` est-elle arrivée à `portable` ? Expliquez.
4. Pour être absolument sûr, faites tourner un `tcpdump` sur chaque interface réseau du poste (option `-i ethN`) : pour cela, décommentez dans le fichier `/etc/inittab` les deux lignes suivantes :  

```
#1:2345:respawn:/sbin/getty 38400 tty1
#2:23:respawn:/sbin/getty 38400 tty2
```

Redémarrez le poste (commande `reboot`) pour obtenir deux consoles. Étudiez attentivement les paquets IP qui passent lorsque le `portable` veut accéder par `ping` (ou `ssh`) à `bighost`. Quels paquets manquent et pourquoi ?
5. Modifiez `/etc/init.d/firewall` (et lancez-le) pour mettre en route le `masquerading`. Quelle différence dans les paquets IP émis/reçus ?
6. Depuis `portable`, effectuez plusieurs `pings` vers `bighost`, avec son nom, son adresse, etc. Expliquez les résultats.

## 5 Redirection de services, DNAT

1. Vérifiez qu'un serveur web tourne bien sur `zbox`, et que vous pouvez le consulter depuis les machines du réseau familial (et bien sûr pas depuis l'extérieur)
2. Complétez et mettez en service les règles de filtrage concernant le DNAT : il s'agit de rediriger les paquets destinés au port 80 de `poste.bignet.com` vers `zbox` port 80 (modification d'adresse du destinataire), et qu'au retour, les réponses semblent provenir de `sweethome` (et non de `zbox`).

## Mémento iptables

### Tables et chaînes prédéfinies

- La table par défaut (**filter**) contient les chaînes prédéfinies **INPUT**, **OUTPUT** et **FORWARD**.  
**INPUT** traite les paquets IP dont la *destination* est locale (une interface de la machine).  
**OUTPUT** traite les paquets IP dont la *provenance* est locale.  
**FORWARD** traite les paquets IP en transit.
- La table **nat** contient les chaînes **PREROUTING** et **POSTROUTING**.  
**PREROUTING** traite les paquets IP dont la destination est locale ainsi que les paquets IP en transit. Les règles de type **PREROUTING** sont appliquées *avant les autres règles*.  
**POSTROUTING** traite les paquets IP dont la source est locale ainsi que les paquets IP en transit. Les règles de type **POSTROUTING** sont appliquées *après les autres règles*.

### Commandes IPTABLES

Voir les règles	<code>iptables -L; iptables -t nat -L</code>
Définir une politique par défaut	<code>iptables -P INPUT DROP</code>
Effacer les règles d'une chaîne	<code>iptables -F OUTPUT</code>
Ajouter une règle	<code>iptables -A FORWARD -s 10.1.1.0/24 -j ACCEPT</code>

### Conditions IPTABLES

Interface	<code>-i eth0</code>	<code>-o ppp0</code>
Adresse IP (source, destination)	<code>-s 10.1.1.0/24</code>	<code>-d 10.1.1.45</code>
Protocole	<code>-p tcp -p udp -p icmp</code>	
Port (avec TCP ou UDP)	<code>--source-port 53</code>	<code>-destination-port http</code>
État de la connexion (avec TCP)	<code>-p tcp -m state --state ESTABLISHED,RELATED</code>	<code>-p tcp -m state --state NEW</code>
Saut vers une cible (action)	<code>-j ACCEPT</code>	<code>-j DROP</code> <code>-j REJECT</code>

### Traduction d'adresse (NAT)

Masquering (SNAT)	<code>iptables -t nat -A POSTROUTING</code> <code>    --source 10.1.1.0/24 -o eth1 -j MASQUERADE</code>
Redirection (DNAT)	<code>iptables -t nat -A PREROUTING -i eth0 -p tcp</code> <code>    --dport 80 -j DNAT --to-destination 10.1.1.2:80</code>