**TD – Routage et iptables**
ING3 – ICC – Sécurité des systèmes d'information
Année 2014–2015


# 1 Réglages initiaux

Assurez-vous du résultat de la commande ci-dessous.

```
# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

Assurez-vous également du résultat de la commande ci-dessous.

```
# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
```

Choisissez une machine sur laquelle vous testerez les requêtes et une autre depuis laquelle vous ferez vos essais de connexion. Retirez les règles testées avant de continuer (sauf celles en gras). Vérifiez à chaque fois ce qui se passe dans Wireshark.

Pour vérifier les règles, vous pouvez taper :

```
iptables [-t nat] -L -n -v
```

# 2 Instructions simples

On suppose ici que votre interface principale est eth0, faites un `$ifconfig` pour vérifier.

1. Interdire tout nouveau paquet entrant par défaut.
2. Rejeter le protocole ICMP.
3. Rejeter le protocole ICMP provenant de localhost.
4. Interdire toute connexion à destination de localhost.
5. Interdire tout paquet qui ne provient pas de localhost.
6. Rejeter un paquet s'il provient de lo.
7. Interdire tout paquet transitant par eth0.
8. Interdire tout paquet extérieur à destination du protocole IPP.
9. Rejeter tout paquet entrant sur eth0 dont le port destination est inférieur à 1024.
10. Interdire toute tentative de connexion UDP en provenance de eth0.
11. Rejeter tout ping entrant.
12. Interdire les réponses à un ping.
13. Bloquer tous les paquets de broadcast entrants sur votre machine.
14. Interdire tout paquet entrant par eth0 dont l'adresse mac n'est pas celle du voisin.
15. Interdire tout paquet entrant par eth0 dont l'adresse mac est celle du voisin.
16. Interdire tout paquet entrant par eth0 dont l'adresse mac et l'adresse IP ne sont pas celles du voisin.
17. Réinitialisez toutes les chaînes et remettez les polices par défaut à ACCEPT.
18. **Positionner maintenant la police par défaut à DROP pour la chaîne INPUT.**
19. Écrire une règle qui laisse entrer 10 tentatives de connexion ping puis n'en laisse passer plus que 2 par seconde.
20. Écrire une règle qui laisse entrer 10 tentatives de connexion UDP puis qui n'en laisse passer plus que 2 par seconde.

21. **Positionnez maintenant les règles par défaut à DROP pour les chaînes INPUT, OUTPUT, FORWARD.**

22. Autoriser en entrée tout paquet en rapport avec une connexion déjà établie préalablement en sortie.

23. Autoriser tout paquet créant une nouvelle connexion en sortie à destination du port 80 en TCP.

24. Que faut il ajouter ici pour que l'on puisse naviguer sur le net ?

25. Créer une chaîne qui log un paquet entrant sur le port 21 en ajoutant le préfixe [INPUT DROP FTP] et qui le drop.

26. Renvoyer vers votre voisin toute connexion entrante sur le port 22.

27. Renvoyer vers le port 8080 de votre voisin toute connexion entrante sur le port 80.

28. Votre machine se met en sécurité (blocage de tous les ports en entrée et en sortie) si quelqu'un tente d'accéder au port 600 de votre machine.

29. Envoyer un mail à votre adresse EISTI si quelqu'un tente d'accéder au port 700 de votre machine.

# 3 Problèmes

(1) Coupez le VPN de votre machine (A). Configurez la machine A pour qu'elle utilise l'autre machine (B) en passerelle et ainsi pouvoir aller sur Internet. Sur la machine B, faites les réglages nécessaires pour que la machine A puisse aller sur Internet.
Une fois que cela fonctionne, modifiez les réglages de la machine B pour que seule la machine A soit autorisée à utiliser la machine B en tant que passerelle. Vous devrez enregistrer en log sur la machine A tous les paquets qui traverseront (un log pour la sortie, un log pour l'entrée). □

(2) Vous voulez protéger votre machine. Faites le nécessaire pour laisser le minimum d'ouvertures en sachant que vous devez impérativement laisser passer les trames ICMP en entrée et en sortie. Pour le reste c'est à vous de voir. Il faudra au minimum pouvoir vous rendre sur Internet via le proxy de l'école.
Faites un script de démarrage pour vos règles et configurez votre machine pour que le script s'exécute au démarrage de votre machine. □

(3) Vous louez un serveur chez un hébergeur. Cette machine est entièrement ouverte, aucun pare-feu n'est installé. Configurez-la au mieux pour qu'elle puisse servir de site Web via les ports HTTP et HTTPS. Elle devra aussi répondre au SSH et au ping. Afin d'éviter les attaques en déni de service, on limitera les demandes ping à 10 par minute après 5 première demandes. De la même manière on interdira plus de 5 demandes par seconde sur le port Web après 5 premières demandes. Tout le reste devra être bloqué. □