TP de Réseaux IP : Sécurité et Firewall

1. *Les architectures de sécurité, firewall*

Cette section est empruntée d'un document sur les Firewalls écrit par A. Dudin et M. Andrès en 2002 pour un sujet bibliographique dans le cadre du DESS IIR option Réseaux de Lyon. Le Firewall ou «coupe-feu » ou encore «garde-barrière » est essentiellement un dispositif qui constitue un filtre entre un réseau considéré comme sûr, tel que le réseau local auquel vous appartenez, et un réseau qui ne l'est pas, tel qu'Internet. Derrière le mot firewall se cache un concept plutôt qu'un matériel ou un logiciel bien défini. Nous dirons qu'un firewall peut être généralement constitué de plusieurs éléments parmi lesquels nous distinguerons:

- Un (des) routeur (s) assurants les fonctionnalités de filtrages.
- Une (des) machine (s) dites «système bastion » qui entre autres assurent les fonctions:
  - de passerelle applicative (proxy) pour les applications les plus connues telles que telnet, FTP, WWW, Mail, etc.
  - D'authentification des appels entrants, avec éventuellement mise en oeuvre de systèmes d'authentification par clé.
  - D'audit/log/trace des appels entrants ainsi que des sessions mail, WWW, etc.

Le rôle d'un environnement de firewall est d'assurer un certain niveau de protection du réseau interne, tout en permettant de travailler sans trop de contraintes. Ceci est possible grâce à des techniques de filtrage de plus en plus rapides et intelligentes.

La mise en activité d'un environnement firewall doit impérativement s'accompagner d'une réflexion à propos de l'objectif que l'on veut réellement atteindre, de la politique de sécurité et d'utilisation du réseau que l'établissement souhaite voir respectée, ainsi que des moyens que l'on est prêt à y mettre. Il faut que la politique de sécurité soit acceptée par tous, sinon, on tentera de la contourner, avec les conséquences que l'on peut imaginer. Ce n'est qu'une fois cette politique définie (dans ses grandes lignes) que le choix de solutions techniques et organisationnelles peut être opéré. Ceci pour dire que ce n'est pas la technologie qui doit imposer une politique de sécurité parce que l'outil est «joli» et le vendeur agréable, mais bien que la politique de sécurité dicte les solutions. De nombreux constructeurs proposent leurs solutions, et parfois, les moins onéreuses ne sont pas les plus mauvaises! D'autre part ce choix devra également prendre en compte le niveau des ressources humaines disponibles, pour l'installation, la configuration et la maintenance du produit! Les produits de sécurité nécessitent un investissement de départ pour l'installation, mais également un suivi constant. L'engagement doit en être pris dès le départ. Ainsi du temps «d'administrateurs compétents et rigoureux» doit être prévu pour le suivi de l'exploitation. Il faut donc trouver une solution adaptée aux besoins, aux moyens, à l'environnement, et à la culture de l'entreprise. Grâce à cette analyse vous pourrez connaître les avantages, les inconvénients ainsi que le fonctionnement des différentes architectures firewall.

2. *Schéma des sous-réseaux*

On réalisera les sous-réseaux en utilisant des hubs. Pour simplicité de lecture, on choisira pour les réseaux R1, R2, R3, R4 et R5 les adresses 192.168.[1- 5].0 avec des masques de 255.255.255.0 (adresse de classe C où le troisième octet permet de spécifier 256 sous-réseaux, on suppose que l'administrateur a reçu 5 adresses de sous-réseaux différentes). L'adresse IP d'une machine sur un sous-réseau s'obtiendra en concatenant son numéro de machine à l'adresse du sous-réseau: par exemple 3 aura l'adresse IP 192.168.1.3 sur le réseau R1. Chaque réseau possède une adresse de diffusion (conventionellement avec les bits de poids

faibles à 1), qui permet de diffuser un paquet IP à toutes les machines du réseau. Dans notre cas on prendra comme adresse de diffusion l'adresse IP du sous-réseau se terminant en 255 (donc pour R2 on a 192.168.2.255).

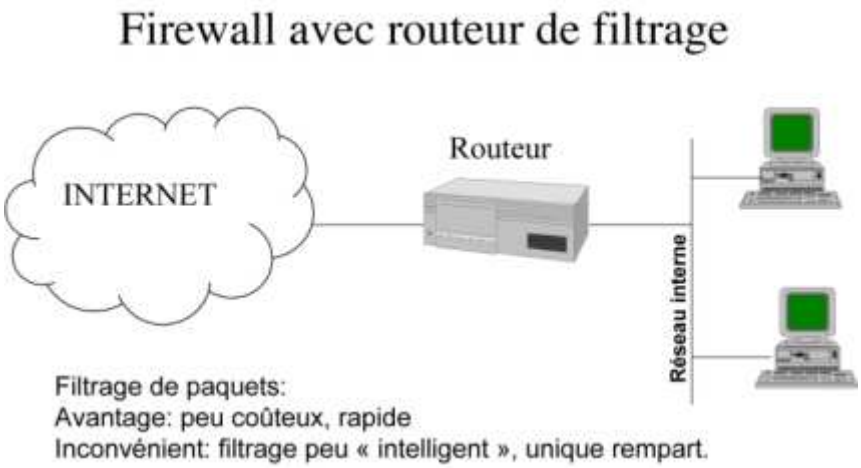


Figure 1: Architecture firewall 1.

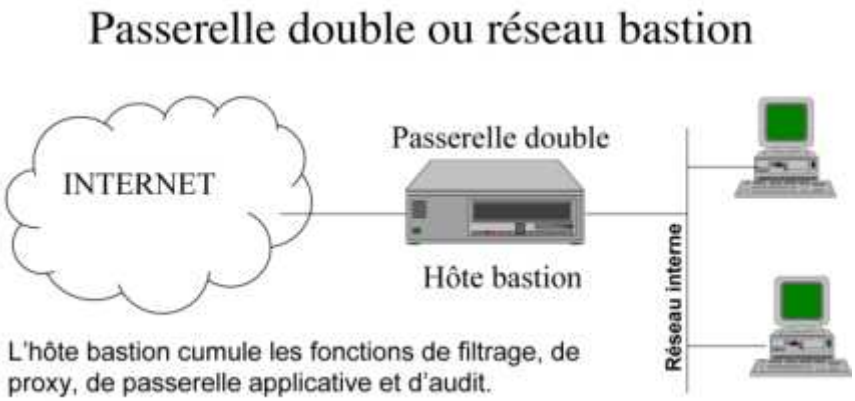


Figure 2: Architecture firewall 2.

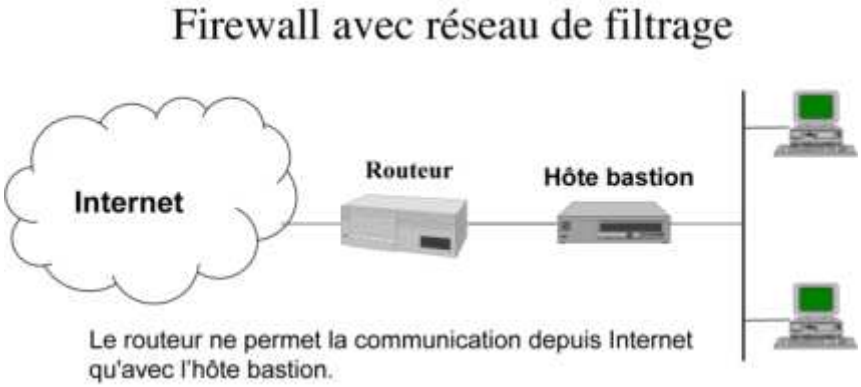


Figure 3: Architecture firewall 3.

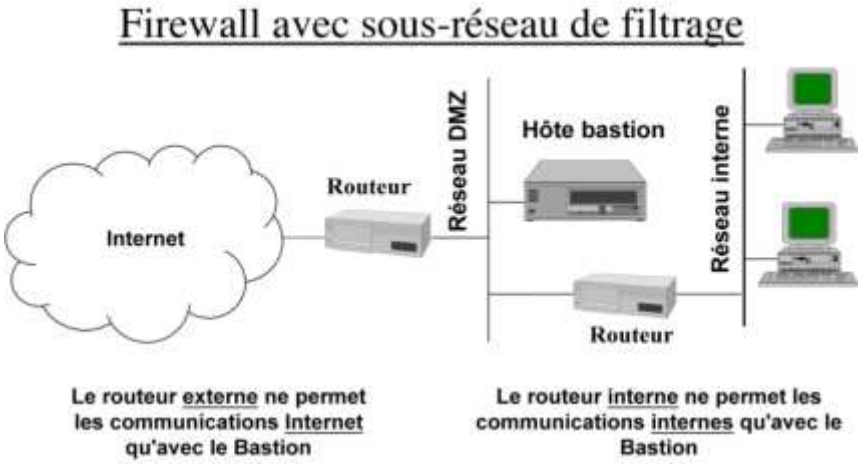


Figure 4: Architecture firewall 4.

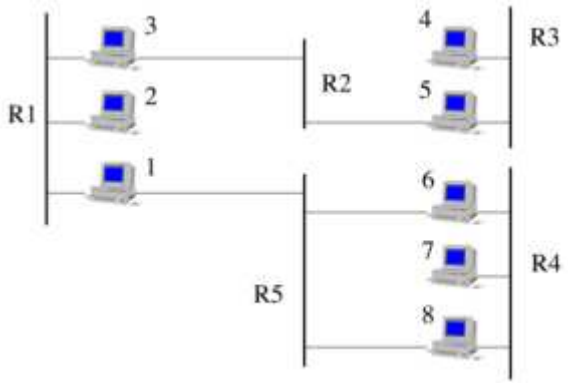
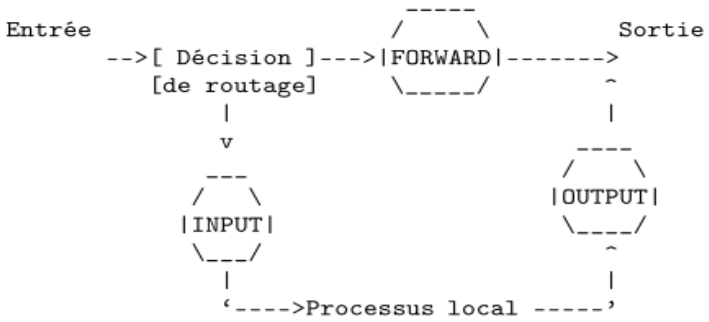


Figure 5: Schéma du réseau.

3. ***Firewall sous Linux***

Le noyeau contient à la base trois listes de règles dans la table "filter"; ces listes sont appelées chaines de firewall ou juste chaines. Les trois chaines sont appelées INPUT,OUTPUT et FORWARD.



La commande iptables (qui remplace ipfwadm et ipchains) permet de spécifier des règles de sélection des paquets IP dans les trois chaînes. Il est également possible de créer d’autres chaînes, mais cela ne sera pas aborder dans ce TP.

Les paquets sont sélectionnés suivant la combinaison : adresse source, addresse destination, protocole (tcp, udp, icmp, all) et numéro de port. Pour chaque règle de

sélection, on peut soit accepter le paquet, soit l'ignorer, soit renvoyer une erreur. Faire man iptables.

Une syntaxe de iptables pourrait être:

iptables -A INPUT -s pn -j DROP pour rejeter toutes les connexions venant de la machine pn.

iptables -I INPUT -s 192.168.1.0/24 -j DROP pour rejeter toutes les connexions venant du réseau R1.

Exercice

Essayer la séquence de commandes suivantes et expliquer le comportement.

ping -i 1 127.0.0.1

[...]

iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP

[...]

ping -i 1 127.0.0.1

[...]

#

Configurer les machines de telle sorte que seules les machines du même réseau ont accès à telnet, plus la machine 3 qui est autorisé pour tout le monde.

Sur les passerelles, interdire le routage des paquets concernant le "portmapper" (port 111 utilisé par exemple par la commande rpcinfo -p <host>.

Vérifier l'efficacité de vos filtres.

4. ***tcpdump***

tcpdump permet de visualiser le trafic TCP sur une station. Faire man tcpdump. Essayer le pour visualiser les mots de passe qui transitent sur le réseau avec les applications rlogin,

ftp...

Exemple: tcpdump -n -x

5. ***ethereal***

ethereal est similaire à tcpdump mais avec une interface Essayer le pour essayer de visualiser les mots de passe qui transitent sur le réseau avec les applications rlogin, ftp...

6. ***Documentation***

En plus des pages de man sur iptables, vous pourrez consulter la documentation en ligne sur

iptableset NetFilter en général. Elle est disponible sur http://www.netfilter.org/documentation/.