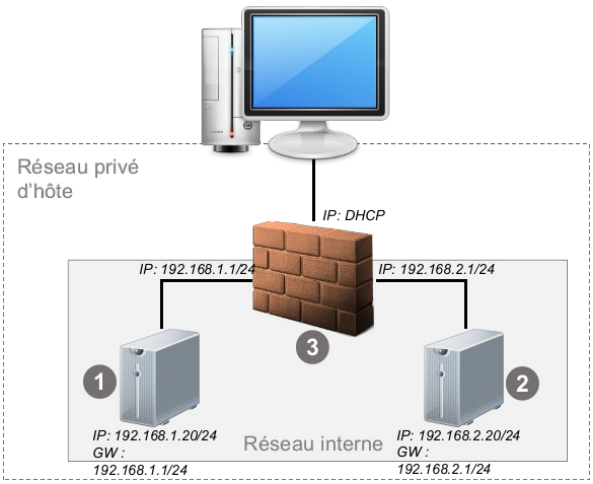
Travaux Pratiques : Netfilter

L'objectif de ce TP est d'appréhender les principes de filtrage des pare-feux (*stateful* et *stateless*) et de connaître les bases de la manipulation de Netfilter..

Installation des machines virtuelles

La configuration de réseau du TP sera la suivante :

Vous avez besoin de trois machines virtuelles : deux serveurs (*1 & 2*) et un pare-feu (*3*), ainsi que deux réseaux de type « réseau interne », pour différencier les sous-réseaux.
Configurez les machines 1 & 2 avec à partir des informations du schéma, leur interface virtualbox doit être définie en « réseau interne » (une par réseau). Le pare-feu dispose de trois interfaces : deux en « réseau interne » (une sur chacun) et une en « pont » ou en « réseau privé d'hôte ».



1 – Configuration initiale

- Activez l'*IP forwarding* sur le pare-feu et faites en sortes que le pare-feu n'autorise aucune communication par défaut entre les équipements, à l'exception de ce qui transite sur l'interface de *loopback* (*lo*).

- Autorisez les flux entrants sur le pare-feu, depuis votre hôte, sur le service SSH. **N'utilisez pas** le module de gestion des états de Netfilter (*-m state*).

- Autorisez les flux SSH entre les machines 1 et 2. Essayez de vous connecter en SSH sur la machine 2, depuis la machine 1 afin de vérifier que cela fonctionne (et inversement).

- Créez un script shell de démarrage */sbin/firewall* contenant les règles Netfilter précédemment définie afin que le pare-feu s'active à chaque démarrage. Ensuite, créez un script de service *systemd* dans */usr/lib/systemd/system/* et activez-le (commande *systemctl*). Vous pouvez vous inspirer de */usr/lib/systemd/system/sshd.service* pour cela.

A partir de maintenant, travaillez directement sur votre script de pare-feu.

- Autorisez tout le monde à se connecter sur le service Apache de la machine 2. Vérifiez que cela fonctionne depuis votre machine hôte. Quel est le problème (et comment le résoudre) ?

- Grâce à Netcat (commande *nc* avec l'options *-p*), connectez-vous au port TCP 22 de la machine 1 depuis la machine 2 en contournant le filtrage en place (vous ne pourrez pas faire de SSH complet car Netcat n'est pas un client SSH, mais il faut juste valider la faisabilité). Qu'est-ce qui explique ce comportement ?

- Modifiez votre script pour que ce ne soit plus possible (en utilisant le module de gestion des états).

- Faites-en sorte que votre script supporte les commandes de type « stop », qui supprime toutes les règles, accepte toutes les connexions par défaut et désactive l'*IP Forwarding* et « restart », qui supprime tout et recharge les règles.

2 – Configuration avancée, journalisation

- Créez une nouvelle chaîne « LOG_DROP » qui permettra de loguer les paquets avant de les droppper. La journalisation doit se faire en préfixant la ligne de log avec « Netfilter DROP: ».

- Créez une nouvelle chaîne « LOG_ACCEPT » qui permettra de loguer les paquets avant de les droppper. La journalisation doit se faire en préfixant la ligne de log avec « Netfilter ACCEPT: ».

- Faites en sorte que le comportement par défaut du pare-feu soit de dropper les paquets qui n'ont pas été explicitement autorisés en les loguant.

- Journalisez l'ensemble des demandes de connexion au serveur web de la machine 2.

- Montrez que cela fonctionne…

3 – Configuration avancée, translation

- Faites en sorte que les machines 1 et 2 ne divulguent pas leur adresse lorsqu'elle dialogue avec l'extérieur, a fortiori avec la machine hôte (en utilisant le *masquerading*).

- Configurez le pare-feu pour que tous le flux qui lui sont adressés, provenant de la mahine hôte et à destination du port TCP 22, soient redirigés sur la machine 1.

- Configurez le pare-feu pour que tous le flux qui lui sont adressés, provenant de la mahine hôte et à destination du port TCP 2222, soient redirigés sur la machine 2.

- Montrez que cela fonctionne…

4 – Configuration avancée, un peu de sécu

- Bloquez les paquets en provenance de la machine hôte qui auraient une adresse IP source dans un des sous-réseaux des machines 1 et 2.

- Limitez les attaques de type brute-force sur le service SSH du pare-feu en mettant en place une restriction sur l'établissement de nouvelle connexions (maximum 5 tentatives autorisées toutes les 3 minutes), en utilisant le module *recent*.

- Utilisez le module *string* pour **rejeter** les paquets à destination du service web (TCP 80) de la machine 2 s'il contiennent la chaîne de caractères « HACK » et vérifiez que cela fonctionne. Il n'est pas recommandé de procéder ainsi pour avoir une protection efficace, pourquoi ?

- Utilisez la table *mangle* pour augmenter de 1 le TTL des paquets transitant par le pare-feu. Quel est l'intérêt de cette manipulation ?