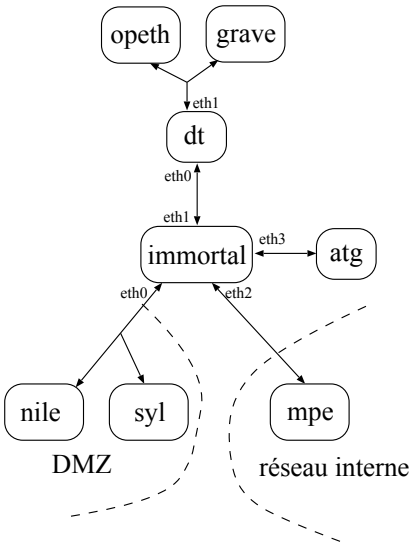
Université Bordeaux — année 2024-2025

Master Informatique/Master CSI — Admin. des Réseaux

TD - Mise en place d'un firewall

Le but de ce TP est de mettre en place un firewall filtrant en utilisant iptables. Il est demandé d'utiliser l'achitecture suivante pour le filtrage :



La topologie réseau peut être obtenue en lançant le script de démarrage `/net/stockage/-aguermou/AR/TP/7/qemunet.sh` en lui fournissant la description de la topologie réseau à l'aide de l'option `-t` ainsi que l'archive contenant la configuration initialte des machines à l'aide de l'option `-a`. Ceci revient à lancer les commandes suivantes :

— au cremi :

```
# cd /net/stockage/aguermou/AR/TP/7/; ./qemunet.sh -x -t topology -a archive_tp7.tgz
```

— à distance :

```
# cd /net/stockage/aguermou/AR/TP/7/; ./qemunet.sh -d tmux -b -t topology -a archive_tp7.tgz
# tmux a
```

L'objectif du TP est de mettre en place un firewall filtrant au niveau de la passerelle `immortal`. La configuration des interfaces réseau et des tables de routages étant déjà faite, il ne vous est demandé que de tester le bon fonctionnement de la configuration fournie dans un premier temps. Remarque : il est nécessaire de tester à chaque étape le bon fonctionnement du filtre à paquets.

1. Faire en sorte que le firewall filtre (bloque) le traffic ICMP vers les machines de la DMZ.
2. Essayez maintenant de pinguer `opeth` depuis `syl`. Commentez et corrigez.
3. Mettre en place une politique par défaut qui interdit tout.
4. Ajouter des règles iptables pour n'autoriser que le traffic sortant du réseau interne vers des serveur http ou ssh. Testez.
5. Ajouter des règles iptables pour que seul les services http et ftp de `syl` soient accessibles depuis les autres machines.
6. Ajouter des règles iptables pour que le service ssh de `nile` puisse être accessible. Raffiner la solution pour faire en sorte que le port 22 de `nile` ne puisse être accessible que depuis `atg`.

7. Ajouter des règles iptables pour que la machine `nile` puisse accéder aux machines du réseau interne via ssh.
8. Ajouter des règles iptables pour que les ports http et ftp de `nile` soient accessibles depuis les machines du réseau interne.
9. Ajouter des règles qui font en sorte qu'immortal n'accepte que 5 ouverture de connexion par minute sur le serveur ssh de `nile`.
10. Mettre en place un mécanisme de traces (logs) qui permet d'avoir un historique de tous les paquets rejetés (DROP/REJECT) au niveau du pare-feu.
11. A l'aide de la commande `nmap`, testez l'efficacité de votre pare-feu.