# M2-Esecure Rezo
# TP: Filtrage

Gaétan Richard, Jean Saquet
Gaetan.richard@unicaen.fr Jean.Saquet@unicaen.fr

23 octobre 2012

## 1 Rappels

On reprend ici le réseaux monté précédemment que l'on va sécuriser.

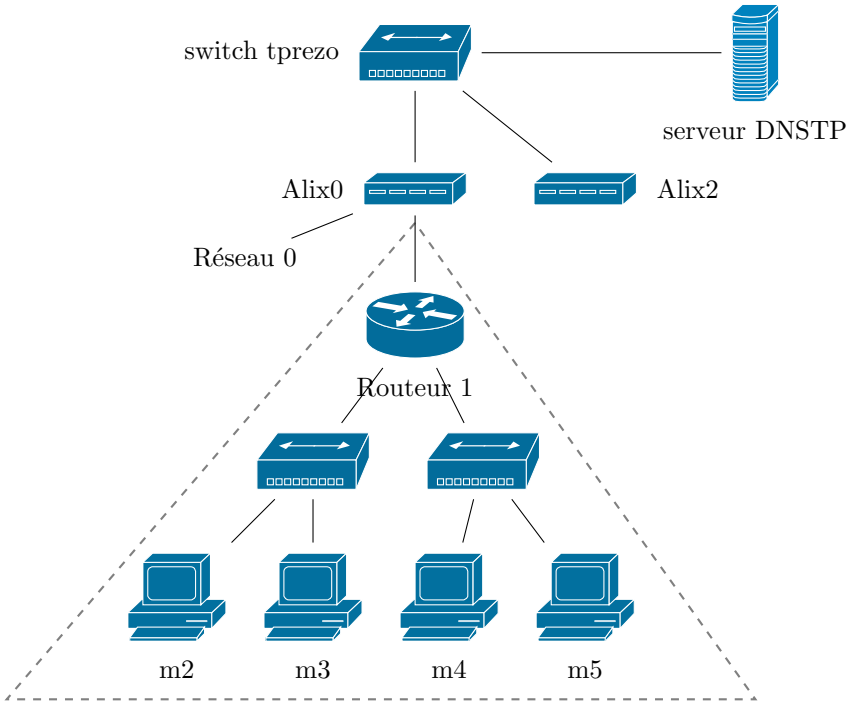


FIGURE 1 – Le réseau avec les ALIX

On utilise les réseaux suivants :
– Interconnexion Alix - Routeur : `192.168.128+48+x.0/24`, `2001:660:7101:ffff:3X::/80` ;
– Réseau `m2` / `m3` : `192.168.32+x.0/24`, `2001:660:7101:2X::/64` ;
– Réseau `m4` / `m5` : `192.168.16+x.0/24`, `2001:660:7101:1X::/64`.
Après avoir relancé les quagga sur les alix, vérifier le bon fonctionnement du réseaux IPv4 et IPv6 .

## 2 Avant de commencer le TP

Pour toute la suite, nous utiliserons **netfilter** que nous manipulerons au travers du programme **iptables**. Vous trouverez une documentation complète sur le site `http://www.netfilter.org/documentation/`.
Nous nous concentrerons principalement sur IPv4 mais la procédure est la même pour IPv6.

# 3 Pare-feu individuel

Dans un premier temps, nous allons nous concentrer sur la réalisation d'un pare-feu de type "individuel" sur la machine m3.

Dans un premier temps, observez l'état du filtrage à l'aide de la commande **iptables -v -L** sur la machine. Nous allons d'abord modifier les politiques par défaut.

## 3.1 Politiques par défaut

Tester différentes politiques parmi `ACCEPT`, `DROP`, pour les chaînes `INPUT` et `OUTPUT`, en regardant à chaque fois le résultat obtenu à l'aide de **ping**, **nmap -p 20-25** et **tcpdump**.

Que faire pour la chaîne `FORWARD` ?

Une fois cette chaîne fixée, nous allons maintenant uniquement travailler sur la chaîne `INPUT` pour le moment la politique par défaut sera `ACCEPT`.

## 3.2 Ajout de règles

Ajouter une règle pour loguer les paquets ICMP entrants. Tester le résultat. Retirer cette règle.

Profiter de cet exercice pour regarder un peu les différentes options disponibles dans iptables. On pourra se reporter à `http://linux.die.net/man/8/iptables`.

## 3.3 Soyons parano

Nous allons maintenant mettre la politique par défaut de `INPUT` à `DROP` et d'ajouter manuellement des exceptions.

Lancer un site web sur m4 puis essayer de le consulter à l'aide de la commande **links**. Quel résultat obtenez vous ?

Corriger ce problème en autorisant les paquets *tcp* appartenant à des connections initiés par l'utilisateur à passer le pare-feu (indice : regardez l'option *-state*). Constater que le problème est bien résolu.

Maintenant essayer de faire **links http ://www/**. Expliquez et corrigez le problème de la même façon que précédemment (pensez à vous souvenir sous quelle forme sont passés les paquets DNS). Est-ce que cela devrait en théorie être possible ?

Pour finir, que ce passe-t-il si on essaie de se connecter à m3 en ssh depuis une autre machine. Faire en sorte d'autoriser les connections ssh mais uniquement depuis la machine m2.

Regarder à l'aide de la commande **netstat -l** quel sont les autres services tournant sur la machine et à l'écoute de l'extérieur.

## 3.4 Et pour finir

Une fois que le pare-feu est en place, faites en sorte qu'il soit sauvegardé lors de l'extinction de la machine et rechargé lors de son redémarrage.

# 4 NAT

Maintenant que nous avons vu les bases, nous allons pouvoir mettre un place un NAT sur la machine Routeur1 afin d'accéder à l'extérieur depuis m4 et m5.

Pour cela, nous allons utiliser la table *nat* et la politique `MASQUERADE`. Une fois la configuration réussie, tester le résultat depuis une autre machine en utilisant par exemple la commande **ping dnstp.info.unicaen.fr**. Est-ce que tout marche correctement ? Expliquer pourquoi.

Maintenant, on souhaiterait que le serveur web soit accessible de l'extérieur. Pour cela, nous allons faire en sorte que les paquets à destination du port 80 de m1 soient redirigés vers la machine www. Ajouter la règle nécessaire et tester le bon fonctionnement.

## 5 Filtrage

Une fois rendu à ce point, peut-on accéder aux machines depuis l'extérieur ? Si c'est la cas, faites en sorte que toutes les connections ssh depuis l'extérieur soient loguées.

## 6 Contourner un pare-feu

Dans les cas où le réseaux est très verrouillé, il est néanmoins possible de contourner un certain nombre de règles par l'intermédiaire de tunnels *ssh*. Cette technique nécessite d'avoir une machine accessible (par ssh) sur lequel vous avez un compte.

Ces tunnels sont crées à l'aide des options **-L** et **-R**. Après avoir lu et relu les descriptifs de ces options, essayez de faire en sorte d'accéder au port *www* de info.unicaen.fr depuis le port 8080 de m2.

Puis rendez accessible le site situé sur m4 depuis un port quelconque sur mike.