M1 Informatique Réseaux et systèmes
TP7: NAT et Filtrage

Gaétan Richard
gaetan.richard@unicaen.fr

10/2017

1 Architecture

Nous reprenons à nouveau le réseau construit dans les TPs précédents (voir figure 1), et nous nous intéressons à la translation d'adresse et au filtrage.

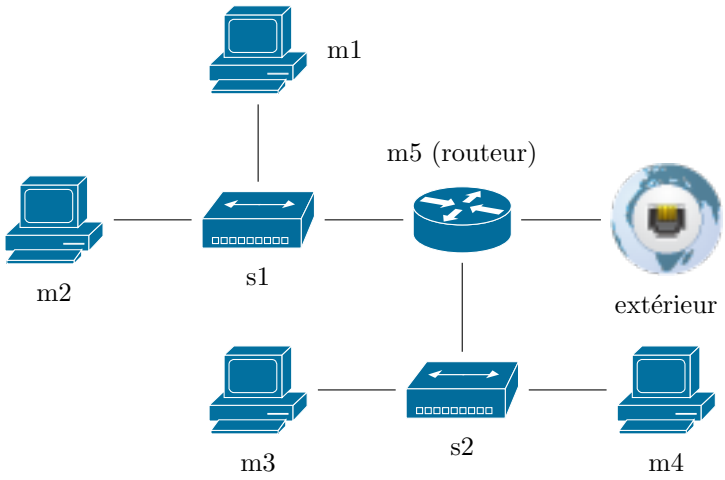

FIGURE 1 – Notre réseau

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

Programmez tout d'abord un service sur m3, par exemple un serveur web en lançant apache : **/etc/init.d/apache2 start**.

Ce service doit normalement être accessible à partir de n'importe quelle autre machine de votre réseau virtuel, puisque le routage interne v4 fonctionne. Vérifiez, par exemple avec **links http ://m3**.

Vous pouvez éventuellement définir ce service dans votre DNS en mettant un CNAME sur la machine m3. Appelez-là "www" par exemple.

Nous allons à présent nous concentrer sur la réalisation d'un pare-feu de type "individuel" sur la machine m3, afin de filtrer les accès à notre service.

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

Testez 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 <no de port>** 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

Ajoutez une règle pour loguer les paquets entrants sur notre service. Tester le résultat. Retirer cette règle.

Profitez 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 ajouter manuellement des exceptions.

Essayez de consulter le service présent sur m3 à partir d'une autre machine. Quel résultat obtenez vous ?

Corrigez ce problème afin d'autoriser l'accès à votre service sur m3.

Maintenant essayez, à partir de m3, de faire une résolution de nom en interrogeant votre serveur DNS sur m2. Expliquez et corrigez le problème en autorisant les paquets *udp* appartenant à des connections initiés par l'utilisateur à passer le pare-feu (indice : regardez l'option *-state*). Constatez que le problème est bien résolu.

Pour finir, que se 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 routeur afin d'accéder à l'extérieur depuis n'importe quelle autre machine.

Pour cela, nous allons utiliser la table *nat* et la politique `MASQUERADE`. Une fois la configuration réussie, tester le résultat depuis m3 ou m4 en utilisant par exemple une requête DNS directement sur le serveur dnstp. Est-ce que tout marche correctement ?

Maintenant, on souhaiterait que le service de m3 soit accessible de l'extérieur. Pour cela, nous allons faire en sorte que les paquets à destination du port choisi pour ce service (80 si serveur web) de m5 soient redirigés vers la machine m3. 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 le cas, faites en sorte que toutes les connections ssh depuis l'extérieur soient logués.

On souhaite isoler les deux sous-réseaux le plus possible. Sur la machine m5, configurez *netfilter* de façon à n'autoriser que le strict minimum entre les deux réseaux. Est-il possible néanmoins de passer d'un réseau à l'autre ?

Essayer de vous connecter sur le port *80* de *www.info.unicaen.fr*. En quoi cela est-il un problème ? Remédiez à la situation.

En vous aidant éventuellement du fichier `/etc/protocols`, réfléchissez à d'autres protocoles à bloquer / autoriser / surveiller.