M2-esecure Rezo
TP4: Serveurs

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

10/2016

1 Introduction

Pour la suite des TPs de réseaux, nous allons construire progressivement une architecture réseaux complète en utilisant les switch disponibles dans la salle, les machines Alix ainsi que des réseaux virtuels via *marionnet*.

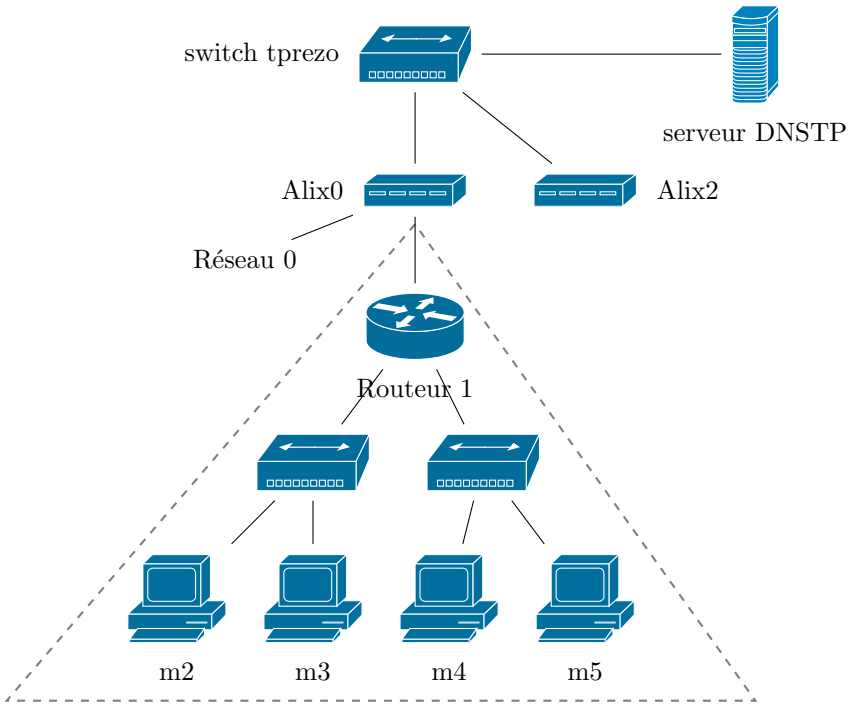

FIGURE 1 – Le réseau avec les ALIX

— 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`.

Dans un premier temps, vérifier la configuration de votre alix et modifier là en conséquence (on prendra l'adresse `1` dans les réseaux d'interconnexion avec les marionnets).

2 Mise en place d'un serveur DNS

Attention : on fera attention pour la suite que le serveur soit bien situé sur la machine `m2` d'adresse `192.128.32+x.2` et `2001:660:7101:2X::2` (on modifiera au besoin l'adresse de cette machine).

Pour toute la suite, le domaine de nom qui vous est attribué est `zone2X.tp.info.unicaen.fr`.

Nous allons maintenant configurer un serveur de nom pour l'ipv4 sur la machine 192.168.32+x.2 (m2) à l'aide de la suite d'utilitaires *bind*. Vous allez maintenant créer ce domaine. Pour cela vous aurez besoin de modifier les fichiers :

— `/etc/bind/named.conf` ;
— `/etc/bind/db.zone2X` ;
— `/etc/bind/db.x+32.168.192` ;
— `/etc/bind/db.x+16.168.192`.
— `/etc/bind/db.2X.7101.660.2001`

Faites en sorte que la machine m2 porte également le nom dnsserver. Vous pouvez alors redémarrer le service par l'intermédiaire du script **/etc/init.d/bind9**.

Une fois ces modifications effectuées, testez le résultat à l'aide des commandes **dig**, **host** et **nslookup**. Penser à modifier le fichier */etc/resolv.conf* pour indiquer le serveur de nom par défaut et le domaine.

3 Serveur Apache

On souhaite installer un serveur apache sur `m3`. Si le package n'est pas installé : installez-le. Ceci nécéssitera peut-être de configurer l'IPv6 ou de mettre un NAT IPv4 sur l'alix.

3.1 Debianneries

Lancez maintenant une machine virtuelle Debian dans marionnet. Observez les différences présentes dans l'organisation du serveur apache dans cette machine. Utiliser de préférence m3. En effet, Debian a décidé par exemple de gérer la configuration de façon un peu différente. Je vous invite en particulier à regarder les commandes a2enmod, a2dismod, a2ensite, a2dissite. À l'aide des outils Debian, configurez le serveur apache en ajoutant au moins un module externe. Observez les processus lancés et leur propriétaire.

3.2 Multiples noms de domaines

Àprès avoir remis en route votre serveur dns, faites en sorte que la machine m4 héberge plusieurs sites : en particulier, on ajoutera un site www.zone2X.tp.info.unicaen.fr et intranet.zone2X.tp.info.unicaen.fr. Pour cette dernière, on fera attention à ce que le site ne soit accessible qu'en interne par protection suivant l'adresse IP.

3.3 Ajout de contenu

Pour rendre le site www un peu plus vivant, nous allons créer : – Une page 404 personnalisé, – Un dossier accessible uniquement par login / mot de passe, – une dossier dans lequel tous le monde peut déposer des fichiers. Pour ce dernier point, on disutera des potentiels problèmes.

3.4 Connection directe

Vous savez qu'il est possible de parler directement au serveur web à l'aide d'une connection TCP sur le port approprié. Pour cela, il vous suffit de connaître le protocole HTTP/1.1 qui est décrit dans la RFC2616. En utilisant telnet, connectez vous à votre serveur et récupérez la page principale de votre site. Faites de même avec info.unicaen.fr, oberservez les cookies et meta-informations du protocole HTTP.

4 Firewall

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 R1 soient redirigés vers la machine www. Ajouter la règle nécessaire et tester le bon fonctionnement.

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.

4.1 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.