Jean-François Berdjugin, Jean-François Remm 2005-2006
IUT1, Département SRC L'Isle d'Abeau

Mise en oeuvre d'un proxy (http)

Il vous faut à ce point du sujet sauvegarder ce fichier sur votre disque dur.

Introduction

Un serveur mandataire ou serveur proxy est un serveur qui a pour fonction de relayer différentes requêtes et d'entretenir un cache des réponses. Un proxy travail au niveau applicatif, il faudrait plus justement parler de proxy http, ftp, ...

Le proxy est foncièrement différent du firewall, ce dernier filtre et modifie les paquets. Le proxy lui est un serveur particulier qui écoute et qui relaye la réponse, aucun paquet ne le traverse.

Un proxy cache peut-être placé n'importe ou sur le réseau et non pas forcement sur un routeur. Si le proxy n'est pas un simple cache, il doit être utilisé conjointement avec un firewall et ou une passerelle NAT (Network Address Translation) pour forcer son utilisation. Le proxy transparent lui doit être obligatoirement placé sur la passerelle NAT.

Un proxy peut être :

- Transparent ou non, si le proxy n'est pas transparent, les clients doivent être configurés pour le prendre en compte,
- Avec ou sans authentification.

Nous allons mettre en oeuvre squid, un proxy http, https, ftp et gopher. Nous l'utiliserons comme proxy http non transparent puis transparent.

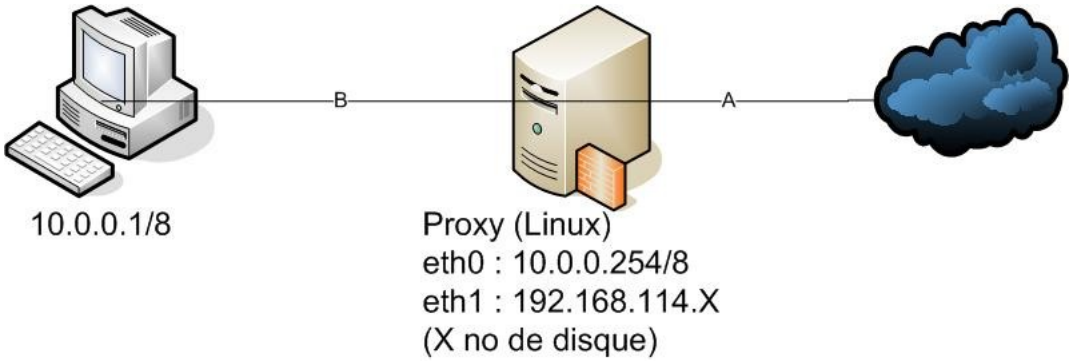
Squid permet aussi :

- l'utilsation de hiérachie de caches (des caches communicants),
- l'utilisation des protocoles ICP (Internet cache protocol), HTCP (Hypertext Caching Protocol), CARP (Cache Array Routing Protocol) et Cache Digests, WCCP (Web Cache Control Protocol) un protocol propriétaire Cisco utilisé par les routeurs de cette marque,
- l'utilisation d'ACL (Access Control List) sophistiquées
- le cache les requêtes DNS.

Installation

Installer si ce n'est pas déjà fait shorewall, squid puis webmin (un assistant graphique de configuration).

Réaliser le câblage suivant :



Pour nous le réseau 10.0.0.0 /8 représentera l'Intranet (loc) et le réseau 192.168.114.0 /24 l'Internet (net).

La machine 10.0.0.1 aura comme routeur par défaut 10.0.0.254 et comme serveur DNS 192.168.114.254. La machine 192.168.114.X aura comme routeur par défaut 192.168.114.254 et comme serveur DNS 192.168.114.254.

Commençons avec une configuration permissive de shorewall. Nous souhaitons mettre en place une passerelle NAT avec les contraintes suivantes : le port 3128 doit être ouvert dans le sens de l'Intranet vers le firewall (fw). Les ports tcp 80 et 3128 doivent être ouverts dans le sens de l'Intranet vers Internet. Le port udp 53 doit être ouvert dans le sens de lIntranet vers l'Internet.
Je vous conseil d'utiliser la méthode suivante :

- Configuration des interfaces (interfaces ») avec un petit piège il vous faudra utiliser l'option no rfc (cette adresse étant privée) sur eth1,
- définition des politiques par défaut (« policy ») avec comme action drop depuis la zone loc vers les autres zones.
- Définition des exceptions (« rules »)
- activation de la translation d'adresse avec « masq ».

Vous pouvez soit utiliser les fichiers de configuration dans /etc/shorewall puis shorewall restart soit l'interface webmin avec « webmin status ». Cette dernière solution offre comme inconvénient de pouvoir être interdite par certaines règles de firewall.

Tester votre configuration en consultant l'URL « http://www.src »

Proxy non transparent

Configurer la machine cliente 10.0.0.1 pour quelle utilise votre proxy sur le port 3128.

Lancer squid soit avec service squid restart soit avec webmin.

Après avoir lancé squid vous pouvez tester depuis le client « http://www.src » vous devez obtenir une page d'erreur.

Pour la suite vous pouvez soit utiliser webmin soit les fichiers de configuration de squid présents

dans /etc/squid.

Création d'ACLs et de restrictions

Créer une ACL de type Client nommée « ACLIntranet » puis une restriction[1] qui autorise le trafic depuis « ACLIntranet ».

Votre test précédant doit maintenant fonctionner (« http://www.src »).

Modifier la configuration de shorewall pour fermer le port 53 (DNS) et le port 53 depuis l'Intranet.

Avec nslooup ou ping vous vérifierez depuis la machine cliente que vous ne pouvez pas contacter le serveur DNS. Alors pourquoi pouvez vous toujours continuer à surfer ?

Les sites de Monsieur Remm étant à caractère subversifs (ils contiennent du java) vous allez interdire la consultation de toutes les urls contenant remm. Pour ce faire il vous faut créer une ACL ACLJFR de type url_regexp contenant l'expression remm puis modifier vos restrictions pour l'utiliser (attention à l'ordre). Tester votre configuration en consultant, depuis la machine cliente, les url suivantes « http://www.src/~jberdjug/ » et « http://www.src/~remm ».

Proxy transparent

Le proxy transparent est un proxy dont le client ne connaît pas la présence, le proxy travail conjointement et sur la passerelle NAT qui relayera tout ce qu'elle reçoit sur le port 80 depuis l'Intranet vers le port 3128 du proxy.

Nous allons commencer par configurer le client web de la machine 10.0.0.1 pour un accès à internet. Puis sur le firewall autoriser le DNS sortant de l'Intranet vers l'Internet.

Tester depuis le client les url http://www.src/~jberdjug/ » et « http://www.src/~remm », elles doivent être accessibles. Nous allons empêcher la consultation des pages subversives en réalisant une translation de port qui transforme tout ports de destination 80 vers n'importe qu'elle adresse en un port 3128 vers l'adresse du proxy.

Depuis le client refaite un test cela ne devrait pas fonctionner car lorsque votre client sait qu'il va rencontrer un firewall, il modifie le paramètre de la requêtre http pour ne pas indiquer seulement un emplacement sur un serveur web mais une url complète. Cette URL est nécessaire au proxy pour retransmettre la requête.

Ne pouvant modifier le client nous allons modifier le proxy, il faut positionner les options :

- HTTP Accel Host : Virtual
- HTTP Accel Port : 80

1 Dans squid le terme restriction n'est pas à prendre au sens strict, une restriction peut être soit une ouverture soit une fermeture portant sur une ACL.

- HTTP Accel Uses Host Header : Yes
- HTTP Accel With Proxy.

Voilà cela devrait marcher.

Comme nous l'avons vu le proxy transparent doit se trouver sur la passerelle et le DNS doit être ouvert ou un serveur cache DNS doit être installé pour l'Intranet. Nous ne l'avons pas vu mais le FTP ne supporte pas le proxy transparent.