

Mise en place d'un serveur proxy

SISR 5

2014/2015



Sommaire

I- Introduction	3
II- Installation d'un serveur proxy	3
III- Administration via interface web	5

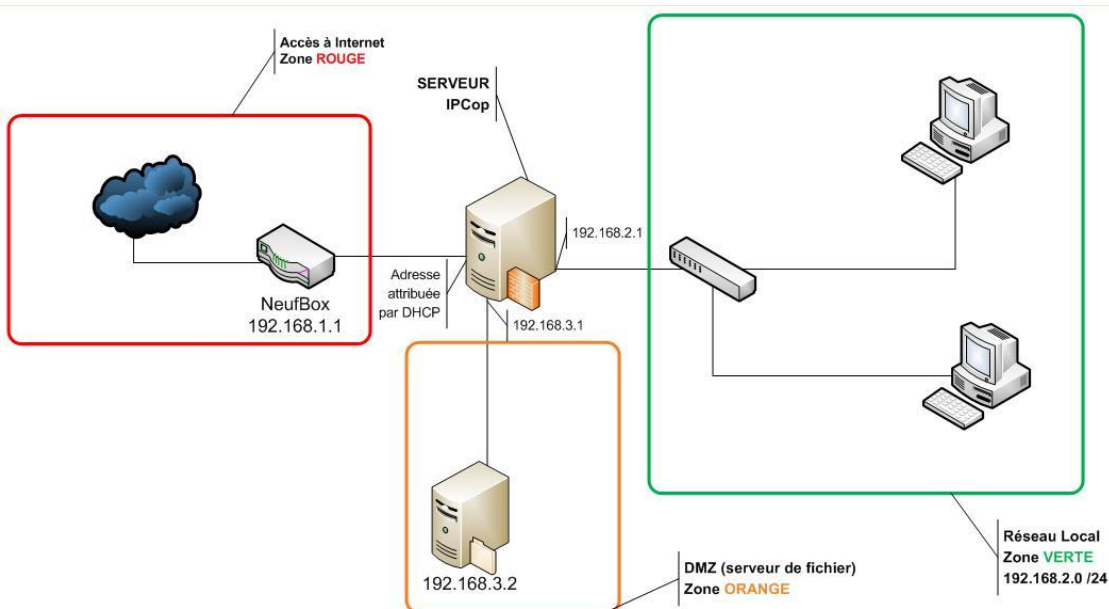
I- Introduction

Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.

Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement internet. Par extension, on appelle aussi proxy un matériel (un serveur par exemple) mis en place pour assurer le fonctionnement de tels services.

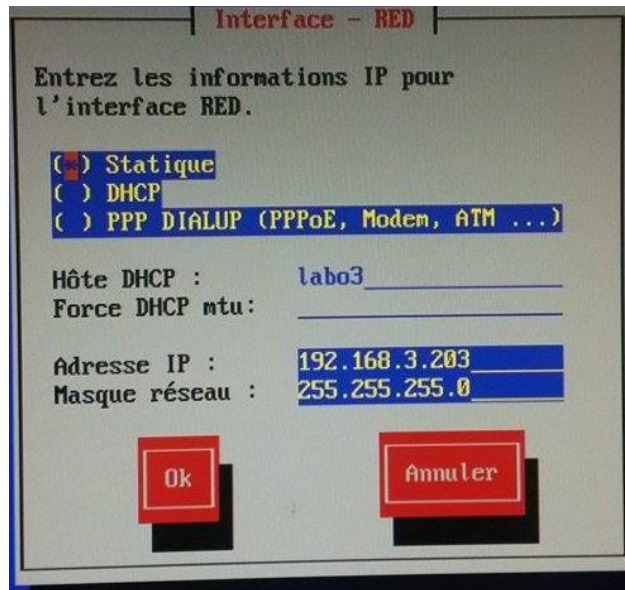
II- Installation d'un serveur proxy

Dans le cadre d'un TP, nous avons mis en place un serveur proxy. Pour cela nous avons utilisé le logiciel "Ip Fire" (IPFire est une distribution Linux, basée sur Linux From Scratch, faisant office de pare-feu.) et nous avons mis en place la solution proxy comme le schéma ci dessous :

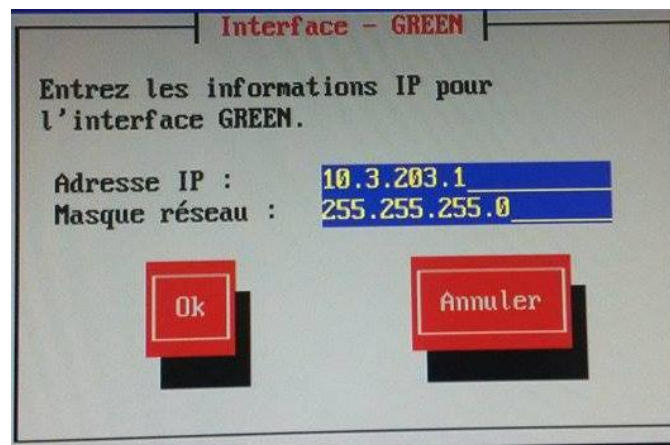


Nous procédons ensuite à la configuration des cartes réseaux, nous choisissons les cartes GREEN (LAN, interne) + RED (WAN, externe). La configuration ORANGE étant pour la DMZ, et la BLUE, pour le WLAN. Le serveur détient donc deux cartes réseau, une pour la GREEN et une pour la RED.

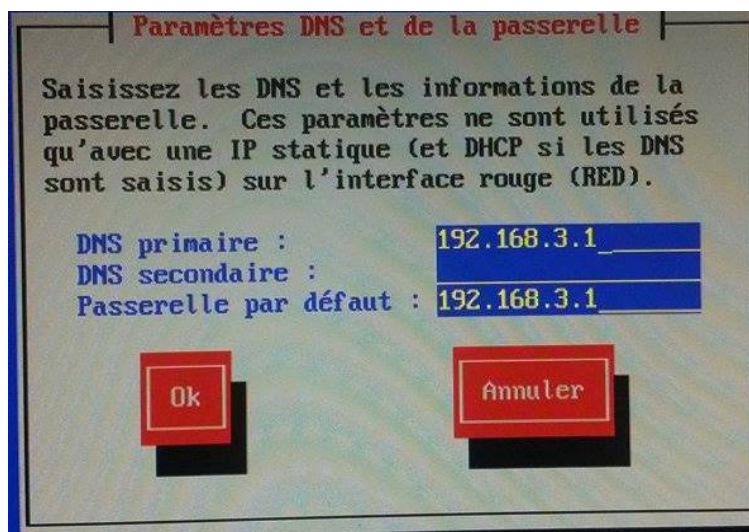
Nous passons ensuite à l'adressage IP des cartes rouges et vertes. L'interface rouge est en statique avec une adresse et un masque correspondant au serveur DHCP du lycée c'est à dire : 192.168.3.x.



Nous procédons ensuite à la configuration de l'interface verte en utilisant le sous réseau de notre labo, ici 10.3.x.x.



Pour finir avec la configuration du serveur, nous renseignons le DNS et la passerelle par défaut correspondant également au serveur DNS du lycée.



Pour finir la procédure d'installation se met en route sur le serveur ce qui nous permet de voir si le serveur est actif et la configuration correcte. Nous renseignons le login et mot de passe paramétrés lors de l'installation du logiciel.

```
Starting DHCP Server...
Starting Apache daemon...
Starting fcron...

IPFire v2.15 - www.ipfire.org
=====
labo3 running on Linux 3.10.44-ipfire i686
labo3 login: root
Password:
Last login: Fri Oct  3 08:48:38 +0200 2014 on tty1.
No mail.
[root@labo3 ~]# _
```

III- Administration via interface web

Le serveur proxy peut gérer les adresses IP grâce à la configuration DHCP. Nous mettons en place cette configuration pour que notre pc portable qui est client puisse détenir une adresse DHCP.

Configuration DHCP

DHCP			
Interface VERTE	Activé : <input checked="" type="checkbox"/>	Adresse IP	10.3.203.1
Adresse de début :	<input type="text" value="10.3.203.11"/>	Masque Réseau :	255.255.255.0
Durée du bail par défaut (minutes) :	<input type="text" value="60"/>	Adresse de Fin :	<input type="text" value="10.3.203.20"/>
Suffixe du nom de domaine : *	<input type="text" value="domlabo3"/>	Durée maximum du bail (minutes) :	<input type="text" value="120"/>
DNS primaire :	<input type="text" value="10.3.203.1"/>	Autoriser les clients bootp :	<input type="checkbox"/>
Serveur NTP primaire : *	<input type="text"/>	DNS secondaire : *	<input type="text"/>
Serveur WINS primaire : *	<input type="text"/>	Serveur NTP secondaire : *	<input type="text"/>
next-server : *	<input type="text"/>	Serveur WINS secondaire : *	<input type="text"/>
		filename : *	<input type="text"/>

* Ce champ peut être vide. Sauvegarder

Pour administrer le serveur via interface web, nous lançons notre navigateur web et nous inscrivons dans la barre URL l'adresse IP de la carte rouge en n'oubliant pas de renseigner le numéro de port 444. Nous retrouvons bien nos deux cartes rouge pour Internet et verte pour LAN.

The screenshot shows the IPFire web interface. At the top, there is a navigation menu with items: Système, Statut, Réseau, Services, Pare-Feu, IPFire, and Rapports. The traffic status is shown as "Traffic: In 0.00 Bit/s Out 0.00 Bit/s". The main content area is titled "Page principale" and contains two tables of network status:

Réseau	Adresse IP	Statut
INTERNET	192.168.3.203	Connecté - (3m 4s)
Passerelle:	192.168.3.1	
DNS Servers:	192.168.3.1	
Réseau	Adresse IP	Statut
LAN	10.3.203.1/24	Proxy éteint

Below the tables, there is a "Note" section with a red background and the text: "Please enable the fireinfo service." At the bottom of the interface, it says "IPFire 2.15 (i586) - Core Update 82" and "IPFire.org • Support the IPFire project with your donation".

Dans ce tutoriel nous essayerons donc différents services proposés par le serveur proxy. Nous commençons donc par activer le proxy web sur l'interface verte pour que nous puissions faire nos essais.

Configuration avancée du proxy Web

The screenshot shows the "Proxy Web Avancé" configuration page. It is divided into "Paramètres communs" and "Informations sur la version supprimée".

Paramètres communs:

- Actif sur Green:
- Transparent sur Green:
- Proxy port: 800
- Transparent port: 3128
- Hostname visible: *
- Langage des messages erronés: de
- Construction des messages erronés: IPFire

Informations sur la version supprimée:

- Squid Cache version: [3.4.5]

Grâce au proxy nous pouvons mettre en place des filtres URL, c'est à dire interdire l'accès à différents sites. Ici dans notre exemple, nous bloquons les sites "materiel.net" et "cdiscout.com".

The screenshot shows the "Paramètres URL filter" configuration page. It includes a "Messages d'erreurs" section and a "Paramètres URL filter" section.

Messages d'erreurs :

Le service Web proxy doit être activé pour utiliser les filtres d'URL

Paramètres URL filter

Bloquer catégories

- ads:
- aggressive:
- audio-vidéo:
- drugs:
- gambling:
- hacking:
- mail:
- porn:
- proxy:
- violence:
- warez:

Blackliste perso

Domaines bloqués (un par ligne) *

Exemple: www.domain.com

http://www.materiel.net/
http://www.cdiscout.com/

URL bloquées (une par ligne) *

Exemple: www.domain.com/ads/

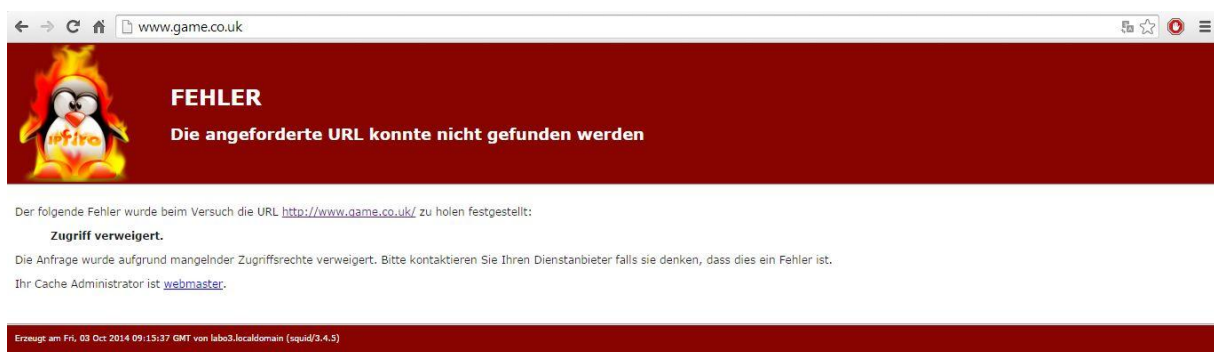
Activer Blackliste perso:

Le blocage des sites peut également se faire par filtrage de mots clés, ici nous utilisons le mot clé "game".

Liste de mots clés perso

Expressions bloquées (comme expressions régulières) *

Nous vérifions donc que le mot à été pris en compte et que nous ne pouvons accéder à aucun site contenant le mot "game". Un message d'erreur s'affiche lors de la recherche, la configuration de filtrage par mots clés à donc bien été pris en compte.



Nous pouvons également activer les rapports du serveur proxy, c'est à dire que nous pouvons récupérer les logs des sites visités.

Configuration des rapports

Rapports activés: Termes de recherche en rapports:
Rapport des robots (de recherche):

Il existe également un service de cache qui est une mémoire qui enregistre des sites, des images afin de diminuer le temps d'accès lors de la prochaine visite du site ou des téléchargements d'images.

Gestion du cache

Activer le gestionnaire de cache:

Cache e-mail administrateur: *

Nombre de descripteurs de fichier: Mot de passe administrateur du Cache: *

Taille cache mémoire (MB): Taille du cache disque dur (MB):

Volume d'objet minimal (KB): Volume d'objet maximal (KB):

Nombre de sous-dossier level-1: Ne pas mettre en cache ces domaines (un par ligne): *

Politique de remplacement de mémoire:

Politique du Cache de remplacement:

Autoriser mode hors connexion:

Enable Cache-Digest Generation:

Le serveur proxy dispose également d'une mise en place de restrictions horaires ou de limitation des téléchargements. Ces dispositifs servent à limiter l'accès sur une période donnée et également limiter le téléchargement à un débit fixé par l'administrateur.

Extensions des Classes Actif:

Restrictions horaire

Accès Lun Mar Mer Jeu Ven Sam Dim De A
autoriser 08 00 16 00

Limites de Transfert

Volume de téléchargement maximal (KB): 0 Volume d'envoi maximal (KB): 0

Contrôle téléchargements

Limite globale Green: 128 kBit/s Limite par hôte Green: illimité
Activer le contenu en fonction de la capacité:
Fichiers Binaires: Images CD: Multimédia:

L'accès aux différents sites peut être autorisés également à différents sous réseaux ou adresses IP. Ici nous autorisons le sous réseau 192.168.3.0/24 à accéder au site sans passer par le proxy. Nous interdisons également l'accès à l'adresse IP 10.3.203.12/24.

Contrôle d'accès réseau

Sous réseaux autorisés (un par ligne):

192.168.3.0/24

Désactiver l'accès du proxy interne VERT vers d'autres sous-réseaux:

Adresses IP sans restriction (une par ligne): *

Adresses MAC sans restriction (une par ligne): *

Adresses IP interdites (une par ligne): *

10.3.203.12/24

Adresses MAC interdites (une par ligne): *

Enfin nous pouvons également rediriger les utilisateurs voulant se connecter vers un site non autorisés par le filtrage proxy, vers un site de notre choix, ici nous avons choisis "google.fr"

Contrôle d'accès basé sur le temps

[Fixer les contraintes de temps](#)

[Fixer quotas utilisateur](#)

URL Filter Réglages

Redirect page template

legacy

Montrer la catégorie de page bloquée:

Redirige vers cette URL: *

http://google.fr

Montrer adresse url page bloquée:

Message ligne 1: *

mauvais site

Montrer adresse IP page bloquée:

Message ligne 2: *

Utiliser "DNS Error" pour les url bloquées:

Message ligne 3: *

Paramètres avancés

Activer liste de mots clés perso:

Activer log:

Activer SafeSearch:

Log identifiant:

Bloquer "pubs" avec fenêtre vide:

Classe les logs par catégorie:

Bloquer sites atteints par leur IP:

Bloquer toutes les url non autorisées explicitement:

Autoriser une liste blanche personnalisée de clients bannis:

* Ce champ peut être vide.

[Sauvegarder](#)

[Valider et Redémarrer](#)