TP : Un proxy TOR/privoxy/squid3 (dans un conteneur LXC, ou pas)

- Objet : Créer un conteneur LXC servant de proxy squid3, protégeant les données personnelles via privoxy et transférant les données via TOR.
- Niveau requis :
  avisé
- Commentaires : *Vous voulez configurer TOR+privoxy pour préserver votre vie privée, le tout derrière squid pour limiter la bande passante et gagner en rapidité.*
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !.
- Suivi :
  en-chantier, à-tester
  - Création par captnfab 02/07/2014
  - Mis à jour par greenmerlin 28/10/2016
  - Testé par <...> le <...> Fix Me!
- Commentaires sur le forum : ici [1)]

Nota :

Contributeurs, les Fix Me! sont là pour vous aider, supprimez-les une fois le problème corrigé ou le champ rempli !

Introduction

- Squid3 est un serveur proxy cache, c'est à dire qu'il garde en mémoire le contenu des images/pages web/feuilles de style/etc. téléchargées de manière à ne pas avoir à les re-télécharger lors d'une nouvelle visite de la page, ou de la visite de celle-ci depuis un autre navigateur du réseau. Les serveurs proxy permettent d'économiser du trafic réseau, ce qui se traduit par un gain de vitesse important sur les réseau lents comme TOR.
- Privoxy est un serveur proxy anonymisant. Il ne fait pas office de proxy cache, c'est à dire qu'il ne mémorise pas les objets téléchargés. En revanche, il filtre les informations envoyées par les navigateurs pour ne laisser passer que le minimum nécessaire.
- TOR est un réseau permettant d'effectuer des requêtes HTTP anonymes sur internet. Cependant, rien n'empêche une machine mal configurée d'envoyer de manière anonyme, une requête HTTP signée de votre nom ou de votre réelle adresse IP. D'où l'intérêt de privoxy.

Prérequis

Pour garder notre système propre, nous n'allons pas installer les serveurs proxy directement sur le système mais dans un conteneur (une sorte de machine virtuel chrooter). Si vous préférez installer cela directement sur votre système, passez au chapitre suivant « Installation des proxy. »

Outils de gestion des conteneurs

Pour cela, nous aurons besoin des outils de gestion des conteneurs.

```
apt install lxc bridge-utils libvirt-bin debootstrap
```

Création d'un conteneur pour les proxy

La création du conteneur se fait très simplement :

```
lxc-create -n proxies -t debian -- -r jessie
```


le -n définit le nom de votre conteneur ici le nom “proxies” sera utilisé

A la fin du traitement le système devrait vous afficher

```
Current default time zone: 'Europe/Paris'
Local time is now:      Fri Oct 28 09:59:59 CEST 2016.
Universal Time is now:  Fri Oct 28 07:59:59 UTC 2016.

Root password is 'gFM0Urj6', please change !
```


Notez le mot de passe sur votre fesse gauche en attendant

Démarrer le LXC et prendre la main

Test de votre conteneur

```
lxc-start -n proxies
```

après le démarrage vous devriez voir

```
Debian GNU/Linux 8 proxies console
proxies login :
```


Regardez votre fesse gauche puis changer le mot de passe root

autre commandes utiles :

Fermer le conteneur

```
lxc-stop -n proxies
```

Démarrage silencieux du conteneur :

```
lxc-start -n proxies -d
```

Obtention d'un shell (root) dans le conteneur :

```
lxc-attach -n proxies
```

Configuration avancée du LXC

Configuration réseau

Par défaut, le conteneur n'aura aucune conf réseau. Se sera à vous de lui en donner une.

Au menu

- SimpleBridge (NAT)
- MasqueradedBridge
- VlanNetworking

Nous ne verrons que le “Pont Simple” dans notre example

Création de l'interface réseaux de pont nommer lxcbr0

```
brctl addbr br0
```

On verifie par

```
ip addr show
```

On ajoute l'interface a “bridger”

```
brctl addif br0 eth0
```

puis on active le pont

```
ifup lxcbr0
```

puis on édite /etc/network/interface pour configurer notre pont de manière permanante

/etc/network/interface

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
```

```
# The primary network interface
allow-hotplug eth0

iface eth0 inet dhcp

# pont réseau
auto lxcbr0
iface lxcbr0 inet dhcp
bridge_ports eth0
bridge_stp off
bridge_fd 0
bridge_maxwait 0
```

Dernier point, modifier la configuration de notre conteneur, on edite le fichier /var/lib/lxc/proxies/config pour remplacer la valeur lxc.network.type = none

/var/lib/lxc/proxies/config

```
...
lxc.network.type = veth
lxc.network.flags = up
lxc.network.link = lxcbr0
lxc.network.name = eth0
lxc.network.hwaddr = 00:16:3e:a3:23:1d //l'adresse MAC vous l'inventez
bien entendu
lxc.network.mtu = 1500
...
```

puis rédemarer votre conteneur pour tester si vous avez le réseau

vous n'avez pas ping d'insatller par default sur votre contener c'est normal, tester plutot avec apt

PAR DEFAULT VOUS AUREZ SYSTEMD CA FONCTIONNE MAL POUR LE MOMENT DONC ON REVIENT A SYSVINIT

```
apt install sysvinit
```

Démarrage automatique de votre conteneur (au boot de votre bécanne)

Simple comme Debian

```
systemctl enable lxc
```

ensuite éditez le fichier /var/lib/lxc/$containername/config

/var/lib/lxc/proxies/config

```
lxc.start.auto = 1
```

puis on vérifie par un

```
lxc-ls --fancy
```

qui vous renvois ça

```
NAME     STATE    IPV4  IPV6  AUTOSTART
----------------------------------------
proxies  STOPPED  -     -     YES
```

Désactiver les recommandations APT

Pour aider les conteneurs à rester minimaux, on peut désactiver le traitement par APT des recommandations comme des dépendances.

/var/lib/lxc/proxies/rootfs/etc/apt/apt.conf.d/00no-recommends

```
APT::Install-Recommends "false";
APT::Install-Suggests "false";
```

Installation de paquets de base

Par défaut, un conteneur est installé avec un système très épuré. Pour ce qui suis, vous voulez probablement installer quelques outils dans le conteneur. Obtenez un shell root dans le conteneur et saisissez par exemple :

```
apt install --no-install-recommends vim-nox nano less aptitude
```

Installation des proxies

On suppose maintenant que l'on est dans un shell root dans notre LXC (ou sur son système si l'on a choisi de ne pas créer de conteneur.)

Installation du proxy Squid comme proxy transparent

Dans un premier temps, nous allons configurer un serveur proxy Squid tout simple.

Installation de squid

```
apt install --no-install-recommends squid3
```

Configuration comme proxy transparent

Ajouter en fin du fichier `/etc/squid/squid.conf` les lignes :

/etc/squid/squid.conf

```
via off
forwarded_for delete
```

Configuration comme proxy pour tout notre réseau

Rechercher et dé-commenter les deux lignes suivantes

/etc/squid/squid.conf

```
acl localnet src 192.168.0.0/16        # RFC1918 possible internal
network
[…]
http_access allow localnet
```

Vous pouvez adapter la première ligne pour qu'elle corresponde au réseau qui doit avoir accès au serveur proxy, par exemple pour un réseau en « 192.168.42.X » :

```
acl localnet src 192.168.42.0/24
```

Vous pouvez également autoriser plusieurs réseaux en rajoutant des lignes similaires :

```
acl voisinnet src 192.168.17.0/24
http_access allow voisinnet
```

Prise en compte de la configuration

```
service squid3 restart
```

Configuration des navigateurs

Ça y est. Il suffit maintenant d'indiquer aux navigateurs d'utiliser localhost:3128 comme serveur proxy. Cela peut également se faire en mettant

```
export http_proxy="http://localhost:3128/"
```

dans le fichier `~/.bashrc`, ou même dans le fichier `/etc/environment`.

Installation du proxy Privoxy

Maintenant, si l'on souhaite que les requêtes sortant de Squid soient « nettoyées » ne nos informations personnelles avant d'aller sur internet, il nous faut (en)chaîner squid et privoxy.

Installation de privoxy

```
apt-get install --no-install-recommends privoxy
```

Configuration de squid pour utiliser privoxy

Rajouter à la fin :

/etc/squid/squid.conf

```
cache_peer 127.0.0.1 parent 8118 0 no-query
never_direct allow all
always_direct deny all
```

Cela indique à squid de passer par le proxy « parent » présent sur 127.0.0.1:8118 (c'est à dire privoxy), et de ne jamais contacter les sites web directement.

Prise en compte la nouvelle configuration

```
service squid restart
```

Et voilà, vos navigateurs utilisant squid3 envoient maintenant leurs requêtes via privoxy.

Installation du client d'anonymisation TOR

Installation de tor

```
apt-get install --no-install-recommends tor
```

Configuration de privoxy pour utiliser TOR

Chercher et dé-commenter la ligne suivante :

/etc/privoxy/config

```
        forward-socks5   /               127.0.0.1:9050 .
```

Prise en compte des modifications

```
service privoxy restart
```

Profit

...

BONUS : Un proxy pour APT

Vous ne voulez probablement pas utiliser TOR pour vos paquets APT. D'une part cela surcharge le réseau, ce qui est mal. D'autre part, ça n'est pas réellement intéressant d'anonymiser le téléchargement de ses mises à jour...

Installer un proxy APT

```
apt-get install apt-cacher-ng
```

Configurer apt

À faire sur toutes les machines de votre réseau :

/etc/apt/apt.conf.d/00proxy-cache

```
Acquire::http::Proxy "http://127.0.0.1:3142";
```

En remplaçant 127.0.0.1 par l'adresse de votre conteneur le cas échéant.

Aller plus loin : sécurisation du conteneur

On suppose ici que l'installation a été faite sur un conteneur ou un serveur dédié à jouer le rôle de proxy.

Si votre serveur proxy est destiné à être utilisé par d'autres utilisateurs que vous, vous pouvez souhaiter changer un peu la configuration. Par exemple, seuls deux ports (deux services) doivent être visibles depuis l'extérieur :

- 3128 (squid3)
- 3142 (apt-proxy-ng)

Deux solutions s'offrent à vous pour vous assurer que les autres services soient invisibles de l'extérieur du proxy.

1. Mettre en place un pare-feu bloquant tous les autres ports
2. Configurer tous les autres services pour n'écouter que sur l'interface locale 127.0.0.1

Tests

- http://checker.samair.ru/
- http://www.proxylists.net/proxyjudge.php

Sources

- http://body0r.wordpress.com/2009/06/24/tor-privoxy-squid-a-little-howto/
- http://forums.debian.net/viewtopic.php?t=59301

1)
N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !

From:
http://debian-facile.org/ - **Documentation - Wiki**

Permanent link:
http://debian-facile.org/atelier:chantier:tp-lxc-squid-privoxy-tor

Last update: **29/10/2016 10:25**