Proxy filtrant avec Squid et SquidGuard

Hainaut Patrick 2013

But de cette présentation

- Présenter le serveur proxy, son utilité et sa mise en œuvre
- Ce type de serveur est très utilisé en entreprise
- Il est donc important d'en comprendre les tenants et les aboutissants

Serveur proxy

- En français, on parle de serveur mandataire
- Un serveur proxy effectue les requêtes Internet (http ou ftp par exemple) à la place de l'utilisateur, ce qui permet:
  - Un partage de connexion internet (rôle de relais, déjà assuré par la passerelle ou le routeur)
  - La mise en cache d'éléments (pages html, images,…)
  - Le filtrage des données
  - La journalisation des requêtes (fichiers logs)
  - La sécurisation du réseau local

Serveur proxy

- Le serveur proxy est fréquemment utilisé dans les entreprises pour filtrer l'accès à internet
- Cela permet d'éviter l'accès à certains sites (facebook, …), au P2P, aux utilitaires de chat (messenger, …)
- Cela permet aussi de garder des traces des sites visités et par qui, ce qui permet de responsabiliser les employés …

Serveur proxy

- Deux modes de fonctionnement:
  - En mode serveur
  - En mode transparent
- En mode serveur, on modifiera les paramètres de connexion du navigateur des postes clients afin d'indiquer l'adresse du serveur et le port sur lequel il doit s'y connecter

Serveur proxy

- En mode transparent, le client ne voit pas de différence sauf s'il accède à un site interdit
- Pas de modification nécessaire sur le poste client
- Les utilisateurs devraient néanmoins être prévenus qu'ils passent par un proxy …

Squid

- Squid est un serveur proxy cache haute performance, qui supporte les protocoles HTTP, FTP, et gopher
- Gopher est une application concurrente au Web qui n'est maintenant plus utilisé que par quelques passionnés
- Contrairement aux serveurs proxy traditionnels, Squid prend en compte toutes les requêtes demandées en un seul processus qui est non-bloquant

Squid

- Squid conserve les données génériques et spécialement les objets très demandés en RAM, il met en cache les requêtes DNS, et implémente le cache négatif lors des requêtes demandées qui ont échouées
- Squid supporte le cryptage SSL (pour les pages internet sécurisées) , une gestion des accès évoluée, et une journalisation complète des requêtes

Squid

- En utilisant le protocole ICP (Internet Cache Protocol), les caches de Squid peuvent être ordonnés selon une hiérarchie , ou par nœud visités pour minimiser la bande passante utilisée par les internautes

Paquetages Squid

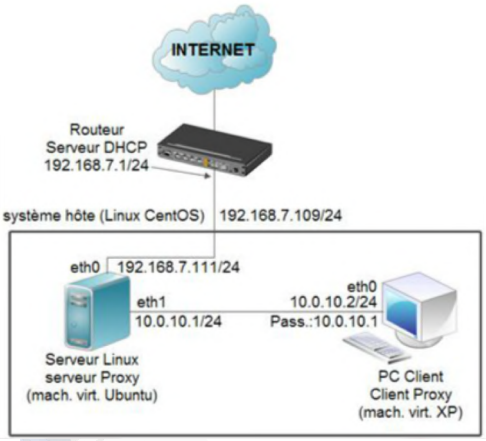
- Les paquetages obligatoires sont **squid** et **squid-common**
- **squidclient** est un utilitaire en ligne de commande qui permet de récupérer les urls dans le cache de squid

Paquetages Squid

- **squidguard** est un filtre, redirecteur et plug-in de contrôle d'accès
- **sarg** est un composant squid qui génère un rapport d'analyse permettant de contrôler « où » vont vos utilisateurs
- **chastity-list** est un composant squidguard contenant la liste noire des sites à interdire

Mise en pratique

Schéma réseau de notre manipulation



Le client passe par le serveur pour avoir accès à Internet et le serveur va filtrer cet accès

Les paramètres IP du coté WAN sont un exemple de ce qu'on pourrait trouver et les paramètres IP du LAN sont un exemple de ce qu'on pourrait configurer

Installation

- apt-get install squid pour la version 2.7
- apt-get install squid3 pour la version 3.x
- Le reste de notre propos concerne squid3

Démarrage – Arrêt

- Pour démarrer le service: /etc/init.d/squid3 start
- Pour stopper le service: /etc/init.d/squid3 stop
- Pour redémarrer le service: /etc/init.d/squid3 restart

Démarrage – Arrêt

- Remarque: pour squid vers. 2.7, la procédure démarrage – arrêt est différente:
  - service squid start/stop/restart
- Seules les options adéquates sont disponibles
  - Exemple: si squid est arrêté, service squid stop renvoie une erreur
- Cette procédure est aussi compatible avec squid3

Démarrage – Arrêt

- Vérifiez par service squid status que squid est bien démarré, car il n'indique pas de message en cas d'erreur de syntaxe
- Pour voir un éventuel message d'erreur, tapez:
  squid –k debug
- Pour squid3, le message d'erreur éventuel est directement indiqué

Démarrage – Arrêt

- Remarque:

  Par défaut, le service Squid attend 30 secondes avant de s'arrêter, le temps que toutes les connexions éventuellement en cours se ferment

Configuration

- Toute la config. se gère au niveau de **/etc/squid3/squid.conf**
- Ce fichier sert de manuel tellement il est commenté
- Le mieux est de faire un backup de ce fichier et démarrer de zéro

```
mv /etc/squid3/squid.conf /etc/squid3/squid.sv
```


Les ACL

- Les ACL (Access Control List), listes de contrôle d'accès, permettent de définir des éléments du réseau sur lesquels ont doit mettre des droits ou des restrictions

Les ACL

- Exemples:
  acl localNet src 10.0.10.0/24
  définit l'étendue du réseau local

  acl facebook dstdomain facebook.com www.facebook.com
  définit les noms de domaines de facebook

  acl work time MTWHF 09:00-17:00
  définit une plage horaire valable pour les jours Monday, Thuesday, Wednesday, THursday, Friday

Les http_access

- Permet d'utiliser les ACL définies ci-avant pour indiquer qui à accès à quoi et à quel moment
- La liste d'http_access est lue séquentiellement par le système et celui-ci s'arrête dès qu'il trouve une correspondance
- Les http_access ayant une action globale (portée all) seront donc placées en fin de liste

Les http_access

- Exemples:
  http_access allow localNet work !facebook
  autorise l'accès à partir du réseau localNet pendant la période work sauf à facebook

  http_access deny all
  ne permet aucun accès
  doit être la dernière règle, sinon les autres règles n'ont pas d'effet

Configuration des clients

- Notre proxy écoute par défaut sur le port 3128
- Dans les options du navigateur client
  - Avancé, Réseau, paramètres pour Firefox
  - Connexions, paramètres réseau pour IE

-> vous renseignez un proxy manuel dont l'adresse correspond à l'adresse de votre serveur (adresse de passerelle des clients) et le port 3128

squid.conf n°1

```
# Temps de shutdown du service
shutdown_lifetime 2 seconds
# Fichier de log de Squid (pour les accès des clients)
access_log  /var/log/squid3/access.log
# port d'écoute
http_port 3128
#acl
acl all src all  ← uniquement pour squid vers. 2.7
acl localNet src 10.0.10.0/24
acl work time MTWHF 09:00-17:00
acl facebook dstdomain facebook.com www.facebook.com
#http_access
http_access allow localNet work !facebook
http_access deny all
```


25

squid.conf n°1

- La directive: shutdown_lifetime 2 seconds permet de réduire le temps d'extinction de squid de 30 à 2 secondes
- La directive: access_log /var/log/squid3/access.log permet de rediriger les logs (fichier journal listant les évènements) dans le fichier acces.log

26

squid.conf n°1

- La configuration est à adapter à votre étendue d'IP locale
- Une fois le fichier sauvé, redémarrer le service squid
- Testez à partir du client XP
- Vous devriez pouvoir accéder à tous les sites sauf facebook (si vous avez bien entré l'adresse du proxy)

squid.conf n°1

- L'heure qui est prise en compte pour la vérification de l'acl est celle du serveur
- Pour la vérifier, utilisez l'instruction **date**
- Pour la modifier; date -s HH:MM:SS
  Exemple: date -s 09:35:00
- Pour changer le jour et l'heure, utilisez:
  date MMJJHHMM Ex.: date 04301300

squid.conf n°1

- Pour squid version 2.7, il faut définir « all »

  -> acl all src all

Nouvelles règles dans le proxy

- 1. Rajoutez une acl qui permette d'utiliser facebook de 12h00 à 12h45 et activez-là
- 2. Obligez les utilisateurs à utiliser Internet Explorer comme navigateur sauf de 12h00 à 12h45
- 3. Interdire tous les sites qui ont dans l'url, la syllabe « jeu »

Nouvelles règles dans le proxy

- 1. acl lunch time MTWHF 12:00 12:45
  …
  http_access allow localNet lunch
  …

Nouvelles règles dans le proxy

- 2. acl IE browser MSIE
  …
  http_access allow localNet work !facebook IE
  …

Nouvelles règles dans le proxy

- 3. acl jeu url_regex jeu
  …
  http_access allow localNet work !facebook !jeu IE
  …

squidGuard

- On peut interdire l'accès à certains sites grâce aux acl mais si on veut un filtrage plus complet, il faut passer par un redirecteur
- Les requêtes vers squid seront redirigées vers squidGuard qui vérifiera si le site demandé n'est pas sur une liste noire avant de l'autoriser

squidGuard - Installation

- apt-get install squidguard
- Pour récupérer la liste noire, il faut utiliser l'utilitaire **wget** qui permet de récupérer du contenu à partir d'un serveur Web ou FTP
- Il faut l'installer: apt-get install wget

squidGuard - Installation

- La liste noire est maintenue à jour par l'université de Toulouse. Pour la récupérer:
  wget ftp://ftp.univ-tlse1.fr/pub/reseau/
  cache/squidguard_contrib/blacklists.tar.gz
- Pour la décompacter: tar –zxvf blacklists.tar.gz
- Attention, le système décompacte le dossier **blacklists** dans le répertoire courant
- Il faut déplacer ce répertoire dans **/var/lib/squidguard/db**

squidGuard - Installation

- On va le placer dans le répertoire db de squidGuard:
  mv blacklists /var/lib/squidguard/db
- Déplacez-vous dans ce répertoire pour vérifier que le répertoire **blacklists** existe bien et qu'il contient bien des sous-répertoires de thèmes interdits comme **adult** par exemple

squidGuard - configuration

- Nous allons d'abord indiquer à squid que nous utilisons squidGuard
- A la fin du fichier **squid.conf**, nous notons:

```
url_rewrite_program /usr/bin/squidGuard
url_rewrite_children 5
```

ce qui permet de rediriger squid vers squidGuard et indiquer le nombre de processus engendré

squidGuard - configuration

- Dans le fichier **/etc/squid/squidGuard.conf**:

```
dbhome /var/lib/squidguard/db/blacklists
logdir /var/log/squid

src reseau {
        ip 10.0.10.0/24
}
```


squidGuard - configuration

```
dest adult {
        domainlist      adult/domains
        urllist         adult/urls
        expressionlist  adult/expressions
        redirecthttp://10.0.10.1/interdit.html
}
```

Remarque: on peut bloquer d'autres thèmes que les sites adultes, allez voir dans le répertoire **/ var/lib/squidguard/db/blacklists** …

Pour certains de ces thèmes, on ne retrouve pas forcément la directive **expressionlist**, la config. est donc à adapter …

squidGuard - configuration

```
acl {
        reseau {
                pass !adult any
        }

        default {
                pass none
        }
}
```


squidGuard - configuration

- Si vous travaillez à partir du fichier **squidGuard.conf** existant, toutes les autres lignes doivent être commentées
- Faites attention aux accolades, un accolade { doit toujours être suivie d'une accolade }
- Une fois le fichier sauvé, il faut redémarrer **squid3** pour qu'il prenne en compte les modifications apportées à **squid.conf** et **squidGuard.conf**

squidGuard - configuration

- Pour éviter des dégradations importantes des performances du système, il faut reconstruire la BD de squidGuard
- Pour cela, tapez:
  squidGuard –C all –d /var/lib/squidguard/db/blacklists

squidGuard - configuration

- Attention que squidGuard doit avoir accès à la base de donnée des sites interdits
- Or, squid et squidGuard sont contrôlés par l'utilisateur proxy
- Il faut donc que l'utilisateur proxy soit propriétaire de la bd
  chown –Rf proxy:proxy /var/lib/squidguard/db
- Il faut redémarrer **squid3** pour prendre en compte cette dernière modification

squidGuard - configuration

- Il reste à créer la page **interdit.html** et à la placer dans le répertoire **/var/www**
- Pour que cette page soit accessible, il faut bien sur qu'un serveur Web (apache2) soit installé

squidGuard - Test

- On peut vérifier que squidGuard tourne correctement en visionnant les logs situés dans **/var/log/squid/squidGuard.log**
- Vérifiez que ce fichier est présent, sinon créez-le, et rendez **proxy** propriétaire de ce fichier
- Redémarrez à nouveau **squid3**

squidGuard - Test

- On peut vérifier que squidGuard tourne correctement avec la commande:

  tail –f /var/log/squid/squidGuard.log

- La ligne **« squidGuard ready for request »** doit être présente
- **Ctrl-c** permet de récupérer la main

squidGuard - Test

- Si des erreurs sont signalées dans **squidGuard.log**, prenez la peine d'examiner ces erreurs et de déterminer ce qui peut causer ces erreurs …
- Bien souvent, c'est une erreur de syntaxe dans **squidGuard.conf** ou une erreur au niveau de la base de donnée (pas présente au bon endroit, pas le bon chemin, une directive qui n'existe pas, …)

squidGuard - Test

- Sur le poste client, essayez de surfer sur www.playboy.com, ça devrait vous renvoyer vers la page interdit.html

squidGuard - Exercices

- 1. Rajoutez deux types de sites interdits: **games** et **gambling** et testez sur le poste client
- 2. Créez un fichier de log pour la section **games** et testez celui-ci
- 3. Permettez à l'ordinateur ayant l'adresse IP se terminant par .2 d'accéder à la liste **games**

Proxy obligatoire

Obligation de passer par le proxy

- Le problème, c'est que si on enlève le lien vers le proxy dans le navigateur, les utilisateurs peuvent de nouveau surfer normalement
- Il faut donc les obliger à passer pour le proxy
- Pour cela, il faut activer quelques règles de firewall

Règles iptables

- Iptables, qui commande le firewall Linux, sera étudié plus en profondeur dans un prochain cours
- On va agir sur la table filter qui permet de contrôler les accès
- On va agir sur la chaine forward, qui contrôle les paquets qui passent par le firewall

Règles iptables

- Les règles seront tapées dans **/etc/rc.local** qui sera exécuté après chaque changement (cd /etc puis ./rc.local)
- Comme on va exécuter plusieurs fois ce fichier, il faut remettre à zéro (flush) les règles iptables pour éviter qu'elles ne soient activées plusieurs fois

Règles iptables

- Pour cela, il faut taper:
  iptables –t nat –F et iptables –t filter –F
- Ces règles seront tapés en début de fichier avant toute autre règle de firewall puisque celles-ci sont exécutées séquentiellement

Politique iptables

- On va dans un premier temps, bloquer tous les paquets qui passent par le firewall

  iptables –P FORWARD DROP

- Exécutez le fichier **rc.local** après sauvegarde et testez avec le navigateur du client, l'accès Internet devrait être coupé (il faut bien sur s'assurer que cet accès était actif avant …)

Autorisation du trafic à partir du serveur

- On va d'abord autoriser le trafic de retour des paquets envoyés, ce qui nous permettra de taper moins de règles:

```
iptables -A FORWARD -m state --state
                ESTABLISHED,RELATED
```

- Remarque: quand la table n'est pas précisée, c'est la table filter qui est sélectionnée

Autorisation du trafic à partir du serveur

- Puis, on va autoriser le trafic TCP (HTTP) et UDP (DNS) à partir de l'adresse du serveur qui est aussi l'adresse du proxy, dans ce cas

```
iptables -A FORWARD -p tcp -s 10.0.10.1 -j ACCEPT

iptables -A FORWARD -p udp -s 10.0.10.1 -j ACCEPT
```

Fichier rc.local

```
…
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables –t nat –F
iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE
iptables –t filter –F
iptables –P FORWARD DROP
iptables -A FORWARD -m state --state
        ESTABLISHED,RELATED
iptables -A FORWARD -p tcp -s 10.0.10.1 -j ACCEPT
iptables -A FORWARD -p udp -s 10.0.10.1 -j ACCEPT
…
```


Test sur le client

- Sauvez le fichier rc.local et exécutez-le
- Testez la connexion internet sur le navigateur du client, Internet devrait être fonctionnel, dans les limites imposées par le proxy
- Enlevez le lien vers le proxy dans la configuration du navigateur client et retestez, Internet devrait être coupé

Proxy transparent

Proxy transparent

- La configuration précédente présente le désavantage de nécessiter une configuration sur le navigateur du client
- On va donc modifier le comportement du proxy et du firewall pour que les paquets soit automatiquement redirigés vers le proxy

Proxy transparent

- Adaptation de la config. de squid:

```
…
# port d'écoute
http_port 3128 transparent
…
```


Proxy transparent

- Adaptation des règles iptables:

```
iptables –t nat –F
iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE
iptables -t nat -A PREROUTING -i eth1 -p tcp
      -m tcp --dport 80 -j DNAT --to-destination 10.0.10.1:3128
iptables –t filter –F
iptables –P FORWARD DROP
```

Proxy transparent

- Le proxy transparent ainsi créé laisse passer le trafic HTTP mais pas le trafic HTTPS
- Rajouter ce qui faut pour autoriser ce trafic

Proxy transparent

- …
  iptables -t nat -A PREROUTING -i eth1 -p tcp
  -m tcp --dport 443 -j DNAT --to-destination 10.0.10.1:3128

Conclusion

- Cette présentation vous aura permis d'aborder le serveur proxy et ses différents modes de fonctionnement
- Il reste encore beaucoup à dire, notamment sur les fichiers logs …
- N'hésitez pas à partir de cette base, à pousser plus loin vos expérimentations, c'est comme cela qu'on apprend le mieux