

# Squid

5 de març de 2016

## 1 Squid com a proxy

S'ha de tenir en compte que quan un navegador es connecta a internet a través d'un proxy es crea una connexió TCP del client cap al proxy i una altra del proxy cap al servidor:

The proxy server MUST signal persistent connections separately with its clients and the origin servers (or other proxy servers) that it connects to. Each persistent connection applies to only one transport link.[2]

Aquestes connexions es poden fer de dues maneres:

- La connexió es fa a través del proxy però els missatges xifrats viatgen encapsulats a través del protocol HTTP.
- La connexió es crea a partir d'una petició CONNECT des del client. El proxy la rep i estableix una connexió TCP cap al servidor.

En el primer l'squid no pot desxifrar els missatges que hi passen per aquests túnels ja que la connexió segura es negocia directament entre client i servidor.

## 2 Squid com a proxy pel tràfic HTTPS

### Connexió HTTPS a través de proxy amb petició CONNECT

Quan un usuari vol accedir a una pàgina HTTPS a través d'un proxy s'hauria de procedir de la següent manera:

1. Usuari envia HTTPS request.
2. Proxy rep la petició. La petició HTTPS porta el mètode CONNECT informant amb qui s'ha de connectar de manera segura el proxy:

opens a TCP tunnel through Squid to the origin server using the CONNECT request method.[1]

3. Es genera un túnel TCP entre el proxy i servidor. Aquest túnel ha de ser segur i s'utilitza el certificat del servidor original per aquesta connexió.
4. Per a que el túnel del clien al proxy també sigui segur necessitem que el proxy tingui un certificat i un parell de claus.

5. L'usuari rep un missatge HTTP de resposta del proxy amb codi 200 informant que el túnel s'ha establert.
6. A partir d'ara el proxy deixa passar paquets HTTPS per ambdues direccions sense interpretar o comprendre els paquets que hi circulen.

#### **Desxifrat de paquets HTTPS des del proxy**

L'Objectiu d'un servidor proxy hauria de ser sobretot donar privacitat als seus usuaris. Squid pot desxifrar els paquets HTTPS que van i venen d'una connexió HTTPS com si fos un *man in the middle* però no hauria de ser així.

### **3 Squid com a proxy transparent per HTTP i HTTPS**

Redirigim els paquets que arriben al firewall als ports on escoltarà l'squid:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 3130
```

Generem el certificat i claus i després configurem squid:

```
http_port 3128 transparent
https_port 3130 transparent cert="/path to server.crt" key="/path to server.key".
```

### **4 Sobre aquest document**

**Copyright© 2016 Juan Aguilera.**

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation;

with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

A copy of the license is included in the section entitled "GNU Free Documentation License".

### **Referències**

[1] <http://wiki.squid-cache.org/Features/HTTPS>

[2] <http://www.ietf.org/rfc/rfc2068.txt>