

## QUESTIONS

2/ #find / -name squid\* -type f \ more

>> cherche les fichiers nommés commençant par squid (donc squid, squid3, squid.conf ...) sur tous le disque depuis la racine et fait une « pause » pour afficher « page par page »

3/ Fichier de configuration de squid

>> squid.conf dans /etc/squid3 (le renommer mv squid.conf squidsav.conf )

4/ Nom du script de lancement de squid et emplacement

>> /etc/init.d/squid3

5/ Le binaire et squid et emplacement

>> /usr/sbin/squid3

6/ Répertoire du cache et emplacement

/var/log/squid3 (fichier cache.log et access.log)

6/ Script de modification du fichier access.log pour conversion « date/heure »

```
GNU nano 2.2.6          Fichier : dateaccess          Modifié
#!/bin/bash
perl -pe 's/^\d+/localtime(%&)/e' /var/log/squid3/access.log > /var/log/squid3/accessdate.log
```

```
root@routeur:/opt# chmod +x dateaccess
root@routeur:/opt#
```

```
root@routeur:/opt# sh dateaccess
```

```
GNU nano 2.2.6          Fichier : accessdate.log
Thu Jun 28 09:17:16 2018.625      214 192.168.2.8 TCP_MISS/200 8849 GET http://www.squid-cache.org/ -$
Thu Jun 28 09:17:17 2018.069      99 192.168.2.8 TCP_MISS/200 3948 GET http://www.squid-cache.org/de$
Thu Jun 28 09:17:17 2018.264     294 192.168.2.8 TCP_MISS/200 29169 GET http://www.squid-cache.org/I$
Thu Jun 28 09:21:05 2018.837      77 192.168.2.9 TCP_MISS/302 1031 GET http://www.google.fr/ - HIER_$
Thu Jun 28 09:21:06 2018.687      55 192.168.2.9 TCP_MISS/200 726 GET http://www.bing.com/favicon.ic$
Thu Jun 28 09:21:07 2018.062      27 192.168.2.9 TCP_MISS/200 859 GET http://ocsp.pki.goog/GTSGIAG3/$
Thu Jun 28 09:21:08 2018.435     522 192.168.2.9 TCP_MISS/200 13545 CONNECT www.google.fr:443 - HIER$
Thu Jun 28 09:21:09 2018.521 240224 192.168.2.8 TCP_MISS/200 14483 CONNECT clientservices.googleapi$
Thu Jun 28 09:21:09 2018.925 240092 192.168.2.8 TCP_MISS/200 4863 CONNECT accounts.google.com:443 -$
Thu Jun 28 09:21:10 2018.751 240079 192.168.2.8 TCP_MISS/200 71938 CONNECT ssl.gstatic.com:443 - HI$
Thu Jun 28 09:21:10 2018.940 240094 192.168.2.8 TCP_MISS/200 52364 CONNECT www.gstatic.com:443 - HI$
Thu Jun 28 09:21:13 2018.906 240078 192.168.2.8 TCP_MISS/200 3777 CONNECT www.google.com:443 - HIER$
```

## PREPARATION ROUTAGE

```
root@routeur:~# nano /etc/sysctl.conf
```

```
# Uncomment the next line to enable packet forwarding for IPv4  
net.ipv4.ip_forward=1
```

```
# Autoriser le NAT uniquement pour le réseau 192.168.2.0  
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth0 -j MASQUERADE
```

( Relancer : service networking restart )

Vérification du routage

```
root@routeur:~# iptables -L -t nat_
```

```
root@routeur:~# iptables -L -t nat  
Chain PREROUTING (policy ACCEPT)  
target      prot opt source                destination  
  
Chain INPUT (policy ACCEPT)  
target      prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target      prot opt source                destination  
  
Chain POSTROUTING (policy ACCEPT)  
target      prot opt source                destination  
MASQUERADE  all  --  192.168.2.0/24        anywhere  
root@routeur:~#
```

## INSTALL/CONFIG/TEST SQUID

**apt-get install squid3**

**configuration de squid**

```
GNU nano 2.2.6 Fichier : /etc/squid3/squid.conf

http_port 3128
visible_hostname proxy-debian.

cache_dir ufs /var/spool/squid3 100 16 256

#ACL
acl host1 src 192.168.2.8
acl host2 src 192.168.2.9
acl monlan src 192.168.2.0/24
acl heures_acces time MTWHF 8:00-18:00
acl refus_site url_regex microsoft.com *()**.com

#REFUS SEPCIFIES
http_access deny host2

#REFUS SITES
http_access deny refus_site

#ACCEPTES LAN
http_access allow monlan heures_acces

#REFUS AUTRES
http_access deny all
```

Relance squid pour une prise en charge des règles

```
root@routeur:~# /etc/init.d/squid3 restart
```

Ou

```
root@routeur:~# /etc/init.d/squid3 force-reload
```

Vérification du statut de squid

```
root@routeur:~# /etc/init.d/squid3 status
```

Lecture du log du cache

```
root@routeur:~# nano /var/log/squid3/cache.log
```

Lecture du log des accès

```
root@routeur:~# nano /var/log/squid3/access.log
```