TP Administration réseaux
STI4A Version 2020-2021. Proxy « Squid ».

SOMMAIRE :

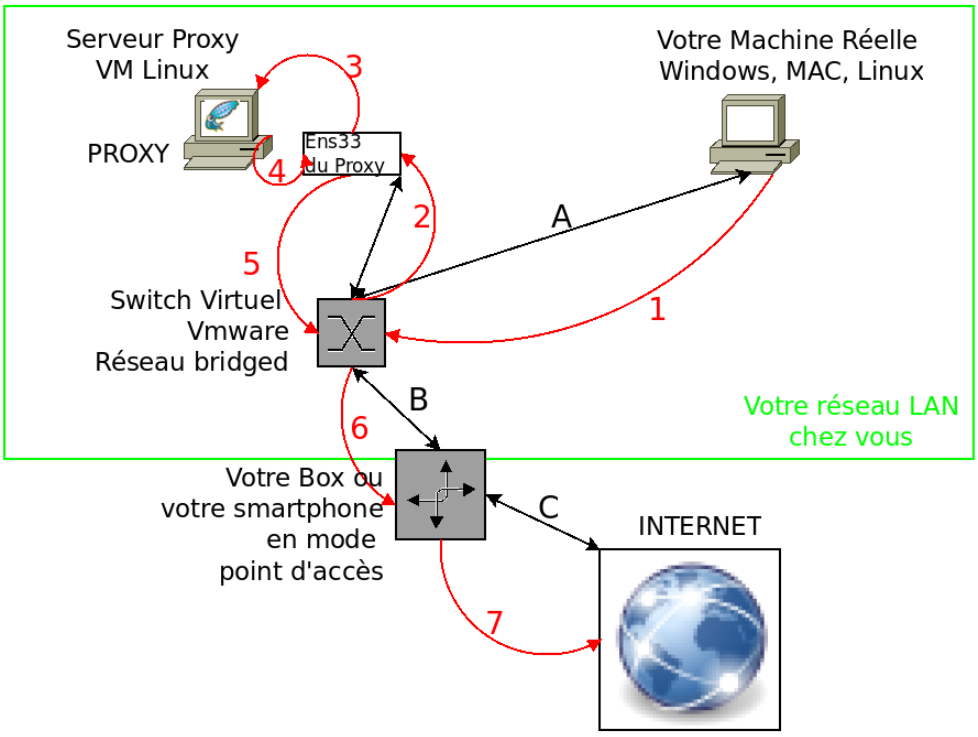
1. Généralités

Le but de ce TP est de mettre en pratique les éléments de théorie vus en cours et de mettre en place et d'administrer un serveur « PROXY » à partir du logiciel libre « SQUID ».

2. Maquette à réaliser

INSA-CVL STI4A
2020-2021

Maquette TD PROXY SQUID

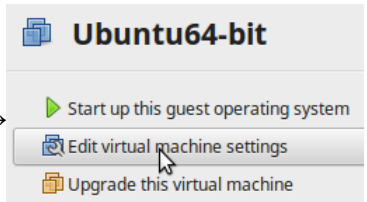


Donc lorsque votre PROXY SQUID sera convenablement configuré, si votre machine réelle émet une requête HTTP ou HTTPS vers INTERNET celle-ci passera par les 7 segments (1..7) en rouge au lieu des 3 segments (A..C) en noir.
De plus le serveur PROXY aura en charge de vérifier après authentification que vous avez un compte utilisateur qui a le droit de le faire.
Pour des raisons d'homogénéité, je vous demande à tous d'utiliser le navigateur « chrome » dans votre machine réelle (Windows , Mac ou Linux).

3. Régler la carte réseau de la machine virtuelle (VM : Virtual Machine).

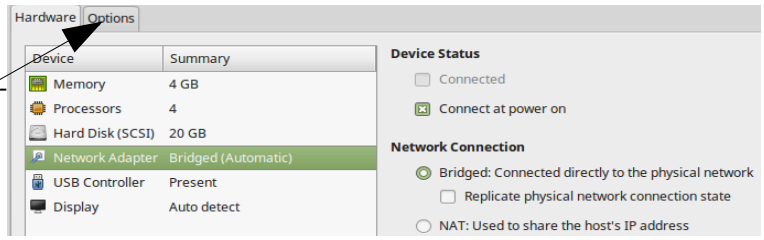
Vous allez utiliser la machine virtuelle que vous avez téléchargée depuis le lien :
https://filesender.renater.fr/?s=download&token=42517e0d-0b8d-4407-b1d2-b8c28c907586
Cette machine, vous devez déjà l'avoir installée dans Vmware Workstation ou Vmware Fusion, pour les utilisateurs de Macintosh. Sinon c'est dommage et faites-le tout de suite.

Votre VM doit être à l'arrêt. Mettez son adaptateur réseau en mode « Bridge ».
Pour cela cliquez sur « Edit virtual machine settings » →



Sélectionnez la ligne « Network Adapter ».

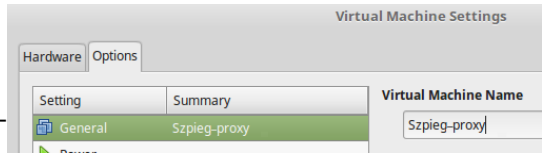
Puis cochez le bouton radio « Birdged » comme ci-contre →



Puis appuyez sur le bouton « Save » :

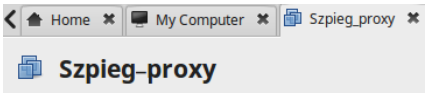
Profitez-en pour personnaliser votre interface « Workstation » ou « Fusion » :
Cliquez dans la fenêtre sur « Virtual Machine Settings » que vous venez d'ouvrir, cliquez sur l'onglet « Options ».

Puis changez le nom de votre Onglet pour votre machine virtuelle :
Vous mettrez « votreNom-proxy » comme ci-contre →



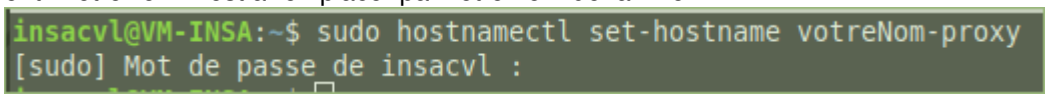
Puis appuyez sur le bouton « Save ».

Résultat →



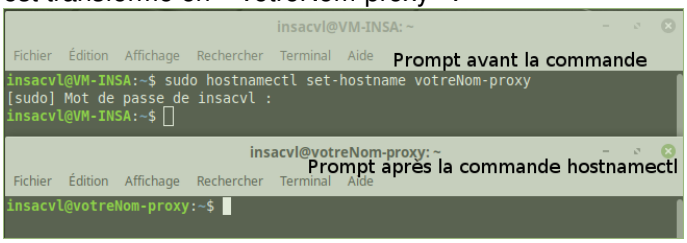
4. Changer le nom d'hôte de la VM « Proxy ».

Démarrer votre VM.
Ouvrez une session avec le compte « insacvl » le mot de passe étant « azerty ».
Lancez un terminal.
Saisissez les commandes de la copie d'écran ci-dessous pour modifier le contenu du fichier « /etc/hostname » et la variable noyau « kernel.hostname » :
Évidemment «votreNom » est à remplacer par votre nom de famille :



Ouvrez un autre terminal. Vous devriez pouvoir vérifier que le « prompt » de « bash » qui contenait « insacvl@VM-INSA » s'est transformé en « votreNom-proxy ».

Résultat :



Fermez la première fenêtre du terminal dans laquelle le « prompt » est « insacvl@VM-INSA ».
Revenez dans le terminal qui est resté ouvert.
Éditez le fichier « /etc/hosts » et mettez à jour le nom lié à l'adresse IP 127.0.1.1→ VotreNom-proxy.
Puis dans le terminal, tapez la commande « clear ». Faites les 5 opérations suivantes :

- En utilisant la commande « sysctl » vérifiez que la variable noyau « kernel.hostname » est bien réglée.
- En utilisant la commande « cat » vérifiez que le fichier « /etc/hostname » a bien été mis à jour.
- En utilisant la commande « cat » affichez le contenu « /etc/hosts » mis à jour par vos soins.
- Faîtes une copie d'écran du terminal en vérifiant bien que les trois informations précédentes sont bien visibles : contenu de « kernel.hostname » ; contenu du fichier « /etc/hostname » et contenu du fichier « /etc/hosts » modifié.
- Nommez cette copie d'écran « 1_hostname.png » et déposez le résultat sur « celene » dans le devoir ouvert à cet effet.

Exemple de copie d'écran« 1_hostname.png » :
Remarque sur ma copie d'écran ci-contre l'attribut de la commande « sysctl » n'est pas visible.
Dans votre copie d'écran ceci ne doit pas être le cas !!

```
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
insacvl@votreNom-proxy:~$ sysctl [redacted]
kernel.hostname = votreNom-proxy
insacvl@votreNom-proxy:~$ cat /etc/hostname
votreNom-proxy
insacvl@votreNom-proxy:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       votreNom-proxy

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
insacvl@votreNom-proxy:~$
```

5. Installer le proxy « Squid » sur la VM « votreNom-proxy ».

Squid est un serveur mandataire (proxy) et un « reverse proxy »conçu pour relayer les protocoles FTP, HTTP, Gopher, et HTTPS (voir vidéo du cours).

Installez squid dans votre VM → Souhaitez-vous continuer ? Réponse « O » bien sûr !!

Remarque :
Si les paquets « squid » ne se chargent pas, tapez « sudo apt update » puis recommencez « sudo apt install squid »

```
insacvl@votreNom-proxy:~$ sudo apt install squid
[sudo] Mot de passe de insacvl :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libdbi-perl libecap3 squid-common squid-langpack
Paquets suggérés :
  libmldbm-perl libnet-daemon-perl libsql-statement-perl squidclient squid-cgi
  squid-purge resolvconf smbclient winbindd
Les NOUVEAUX paquets suivants seront installés :
  libdbi-perl libecap3 squid squid-common squid-langpack
0 mis à jour, 5 nouvellement installés, 0 à enlever et 607 non mis à jour.
Il est nécessaire de prendre 3 277 ko dans les archives.
Après cette opération, 12,5 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

6. Vérifier le bon fonctionnement de « squid » !

6.1. Vérification du service.

Comme « Squid » est qualifié de « DAEMON », (rétro acronyme Disk And Execution MONitor), en 2020 on utilise le terme de service, il n'a rien écrit sur l'écran lors de son démarrage.
Aussi pour vérifier son bon fonctionnement on a deux possibilités :

- Regarder les fichiers de logs.
- Utiliser la commande « systemctl » car on est sur une distribution utilisant « systemd pid=1» (système d'initialisation) au lieu de (initd) plus ancien.

Vous allez prendre la seconde solution et tapez la commande ci-contre → !
« Ctrl+C » pour arrêter la commande.

```
insacvl@votreNom-proxy:~$ systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated)
   Active: active (running) since Mon 2020-11-09 13:41:01 CET; 18min ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 4 (limit: 4630)
   CGroup: /system.slice/squid.service
           ├─5610 /usr/sbin/squid -YC -f /etc/squid/squid.conf
           ├─5612 (squid-1) -YC -f /etc/squid/squid.conf
           ├─5619 (logfile-daemon) /var/log/squid/access.log
           └─5623 (pinger)

nov. 09 13:41:01 votreNom-proxy systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x...
nov. 09 13:41:01 votreNom-proxy squid[5569]:  * Starting Squid HTTP Proxy squid
nov. 09 13:41:01 votreNom-proxy squid[5610]: Squid Parent: will start 1 kids
nov. 09 13:41:01 votreNom-proxy squid[5610]: Squid Parent: (squid-1) process 5612 started
nov. 09 13:41:01 votreNom-proxy squid[5569]:    ...done.
nov. 09 13:41:01 votreNom-proxy systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
```

Faites une copie d'écran de votre résultat, comme ci-dessus, et déposez-la sur « celene » sous le nom « 2_squidStatus.png ». Remarque : le prompt « bash » doit apparaître dans votre copie d'écran, il en est de même pour toutes les copies d'écran qui suivent !

6.2. Quel port le serveur « Squid » utilise-t-il ?

Vous connaissez tous la commande « netstat », donc vous allez vérifier le port serveur de Squid :

```
insacvl@votreNom-proxy:~$ sudo netstat -atnp|grep squid
tcp6       0      0 :::3128                 :::*                    LISTEN      5612/(squid-1)
```

7. Configurer le serveur « Squid ».

« Squid » possède de nombreuses options de configuration, pour cette première approche d'un serveur PROXY vous allez utiliser un fichier minimaliste.

7.1. Faire un « backup » du ficher de configuration d'origine.

Sauvegardez le fichier « squid.conf » original en tapant cette ligne de commande :

```
insacvl@votreNom-proxy:~$ sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.org
```

7.2. Configuration du serveur « Squid ».

7.2.1. Vérifiez l'adresse IP de votre carte réseau « ens33 ».

```
insacvl@votreNom-proxy:~$ ifconfig "ens33"
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.53  netmask 255.255.255.0  broadcast 192.168.1.255
```

7.2.2. Fichier « /etc/squid/squid.conf ».

En tenant compte du résultat obtenu au paragraphe 7.2.1, modifiez le contenu du fichier « /etc/squid/squid.conf » et remplacez son contenu par les lignes suivantes :

```
http_port 3128
visible_hostname  ProxyVotreNom
acl homenetwork src 192.168.1.0/24
http_access allow homenetwork
cache_mem 1024 MB
maximum_object_size_in_memory 1024 KB
memory_replacement_policy heap LFUDA
cache_replacement_policy heap LFUDA
cache_dir aufs /var/spool/squid 10240 16 256
```

Vous trouverez ce fichier « squid.conf » sur « celene », cela vous évitera de le retaper.

Redémarrez « squid » →

```
insacvl@votreNom-proxy:~$ sudo systemctl restart squid
```

Attention : Le service « Squid » va prendre un certain temps à démarrer, c'est normal, soyez patient !!!
En attendant, sauvegardez votre fichier « /etc/squid/squid.conf » sur « celene » sous le nom « 3_squidConf.txt »

7.2.3. Vérifiez que « Squid » fonctionne correctement.

- Avec la commande « systemctl »

```
insacvl@votreNom-proxy:~$ systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated)
   Active: active (running) since Mon 2020-11-09 14:46:22 CET; 6min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 6260 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
  Process: 6285 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
    Tasks: 4 (limit: 4630)
   CGroup: /system.slice/squid.service
           ├─6329 /usr/sbin/squid -YC -f /etc/squid/squid.conf
           ├─6334 (squid-1) -YC -f /etc/squid/squid.conf
           ├─6335 (logfile-daemon) /var/log/squid/access.log
           └─6336 (pinger)

nov. 09 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/
nov. 09 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/
nov. 09 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/
nov. 09 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/
nov. 09 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/
nov. 09 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/
nov. 09 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/
nov. 09 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/
nov. 09 14:46:22 votreNom-proxy squid[6325]: Squid Parent: (squid-1) process 6328 exited with status 0
nov. 09 14:46:25 votreNom-proxy squid[6329]: Squid Parent: (squid-1) process 6334 started
```

- En ne faisant pas confiance à la commande « systemctl » !

La commande « systemctl »est intéressante car en plus du « status » du service elle vous donne un extrait des logs qu'elle va chercher dans le fichier « /var/log/syslog ». Ce n'est qu'un extrait et donc si le service est bavard il manque des informations.

Regardez les logs comme ci-dessous :

```
insacvl@votreNom-proxy:~$ sudo cat /var/log/syslog|grep squic
```

```
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/01
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/02
Nov  9 14:46:22 votreNom-proxy (squid-1): #011Failed to verify one of the swap directories, Check cache.log#012#011for details.  Run 'squid -z' to
create swap directories#012#011if needed, or if running Squid for the first time.
Nov  9 14:46:22 votreNom-proxy squid[6329]: Squid Parent: (squid-1) process 6331 exited with status 1
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/03
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/04
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/05
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/06
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/07
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/08
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/09
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/0A
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/0B
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/0C
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/0D
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/0E
Nov  9 14:46:22 votreNom-proxy squid[6285]: 2020/11/09 14:46:22 kid1| Making directories in /var/spool/squid/0F
Nov  9 14:46:22 votreNom-proxy squid[6325]: Squid Parent: (squid-1) process 6328 exited with status 0
Nov  9 14:46:25 votreNom-proxy squid[6329]: Squid Parent: (squid-1) process 6334 started
```

Tenez compte de l'information « #011Failed » qui apparaît. Exécutez la recommandation dans un terminal (voir liste à puces « Attention » ci-dessous. Faites une copie d'écran du contenu du terminal quand vous avez exécuté la commande indiquée dans la capture d'écran ci-dessus et déposez-la avec le nom « 4_spool.png ».

Attention !! :

- La commande pour arrêter « Squid » peut prendre un certain temps.
- La commande indiquée dans la capture d'écran ci-dessus nécessite, à la fin de son exécution, d'appuyer sur la touche « Entrée » pour récupérer la main sur le terminal.
- La commande qui redémarre « Squid » doit alors être rapide.

Vérifiez dans les logs que cette fois-ci l'information « #011Failed » n'a pas été générée et avec la commande « netstat » que « squid » fonctionne !!.

8. Récupérer l'adresse IP de la machine réelle.

Si vous êtes sous « Windows » lancez « PowerShell » puis tapez la commande « ipconfig ».
Si vous êtes sous MAC OS, ouvrez un terminal dans votre machine réelle puis tapez « ifconfig »
Récupérez l'adresse IPv4 sur la carte « Ethernet » ou la carte « Wifi » suivant la manière dont vous vous connectez à Internet.

Ci-dessous une copie d'écran avec la valeur que j'obtiens chez moi →

```
PS C:\Users\kat18> ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . : home
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.45
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.1.1
```

Remarque : l'adresse IP doit être dans le même réseau que l'adresse du paragraphe 7.2.1. Si ce n'est pas le cas, il y a un problème !

Notez l'adresse IPv4 obtenue dans « PowerShell » sur un papier.

9. Activer la capture de trames sur la VM « VotreNom-Proxy ».

Retournez dans la « VM » « VotreNom-Proxy » et dans un terminal tapez la commande suivante :

```
insacvl@votreNom-proxy:~$ sudo tcpdump host 192.168.1.45 -w proxycap.pcapng
[sudo] Mot de passe de insacvl :
tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
```

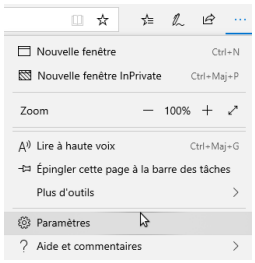
Dans cette commande, l'adresse IP est celle de votre machine réelle que vous avez récupérée au paragraphe 8

Et laissez cette commande « tcpdump » tourner !!!

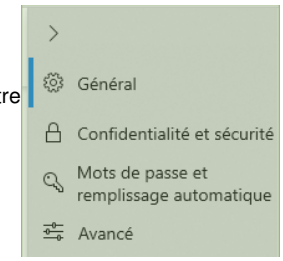
10. Régler « Chrome » sur votre machine réelle.

Je vais le faire sur ma machine avec l'OS « Windows 10 », ceux qui ont un autre OS (Windows seven, OSX, …) peuvent procéder de la même manière :

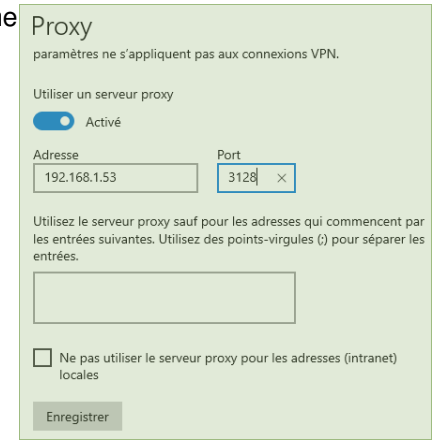
Lancez « Chrome » puis allez dans son menu « ... » en haut à gauche et choisissez « Paramètres ».

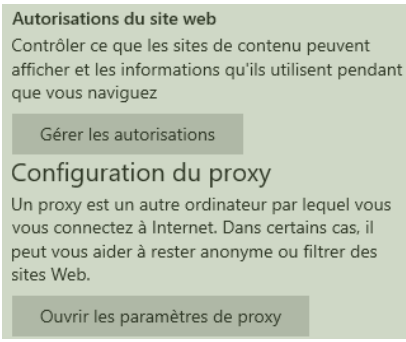


Dans le volet qui s'ouvre choisir « Avancé ».
Attention : Suivant la version de chrome l'interface peut être différente, il faut trouver le réglage proxy !!



Puis descendez grâce à l'ascenseur jusqu'à voir « Configuration du Proxy ».
Cliquez sur ouvrir les paramètres du proxy.
Puis dans la fenêtre qui s'ouvre remplir comme suit :



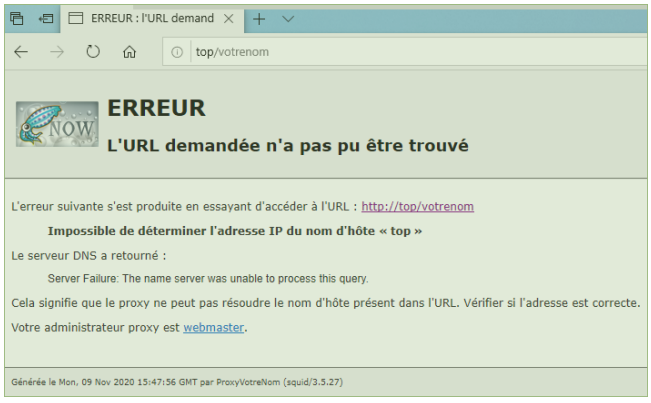


Puis cliquez sur « enregistrer ».

11. Se connecter à une machine non existante.

Dans chrome tapez l'URL suivante : http://top/votrenom

Vous devriez obtenir ceci →



En conclusion votre serveur proxy fonctionne. Vous devez voir votre nom en bas de la page.

Faites une copie d'écran comme ci-contre appelez-la « 4_urlnotfound.png » et déposez-la sur « celene ».

12. Arrêter la capture des trames.

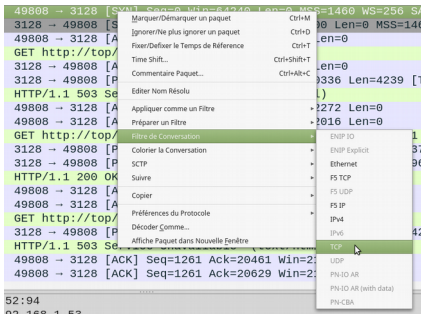
Retournez sur la VM Proxy et arrêtez « tcpdump » en appuyant sur « Ctrl-c »

```
insacvl@votreNom-proxy:~$ sudo tcpdump host 192.168.1.45 -w proxycap.pcapng
[sudo] Mot de passe de insacvl :
tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
^C1005 packets captured
1005 packets received by filter
0 packets dropped by kernel
```

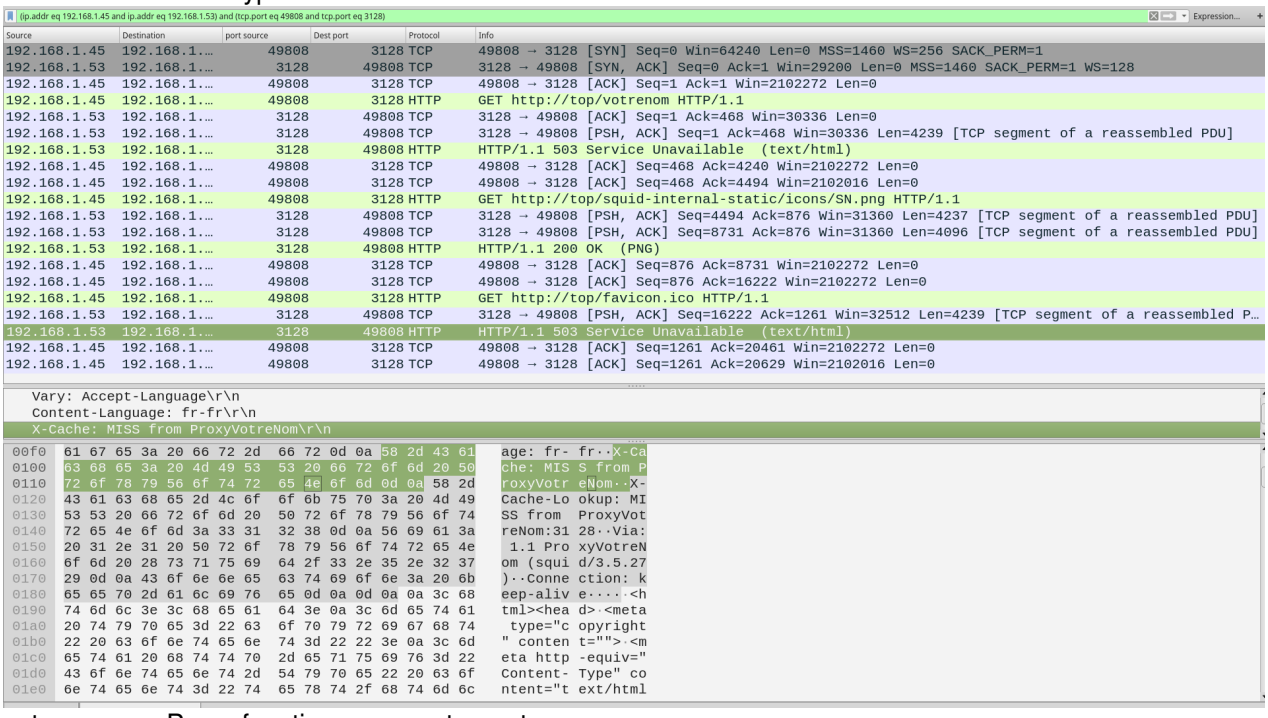
Sauvegardez le fichier « proxycap.pcapng » sous le nom « 5_ proxycap.pcapng » et déposez-le sur « celene ».

13. Étude des trames capturées

Récupérez le fichier « proxycap.pcapng » sur votre machine réelle, et ouvrez-le avec « wireshark ».
Dans la zone « Display Filter » tapez « tcp.port==3128 ».
Vous pouvez aussi, mais pas obligatoirement, filtrer en utilisant les filtres de conversation comme je l'ai fait ci-dessous.
Pour cela recherchez l'un des paquets TCP du « Three-way handshake » de la conversation gérant l'accès à l'adresse « http://top/votrenom ».
Cliquez dessus avec le bouton droit de votre souris puis « Filtre de conversation » et enfin « TCP » comme sur la capture d'écran ci-contre →
Remarque : Si vous n'arrivez pas à filtrer la conversation, faites une copie d'écran sans le filtre !!



Si vous obtenez ce type de résultat :



Source	Destination	port source	Dest port	Protocol	Info
192.168.1.45	192.168.1.…	49808	3128	TCP	49808 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.1.53	192.168.1.…	3128	49808	TCP	3128 → 49808 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
192.168.1.45	192.168.1.…	49808	3128	TCP	49808 → 3128 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
192.168.1.45	192.168.1.…	49808	3128	HTTP	GET http://top/votrenom HTTP/1.1
192.168.1.53	192.168.1.…	3128	49808	TCP	3128 → 49808 [ACK] Seq=1 Ack=468 Win=30336 Len=0
192.168.1.53	192.168.1.…	3128	49808	TCP	3128 → 49808 [PSH, ACK] Seq=1 Ack=468 Win=30336 Len=4239 [TCP segment of a reassembled PDU]
192.168.1.53	192.168.1.…	3128	49808	HTTP	HTTP/1.1 503 Service Unavailable (text/html)
192.168.1.45	192.168.1.…	49808	3128	TCP	49808 → 3128 [ACK] Seq=468 Ack=4240 Win=2102272 Len=0
192.168.1.45	192.168.1.…	49808	3128	TCP	49808 → 3128 [ACK] Seq=468 Ack=4494 Win=2102016 Len=0
192.168.1.45	192.168.1.…	49808	3128	HTTP	GET http://top/squid-internal-static/icons/SN.png HTTP/1.1
192.168.1.53	192.168.1.…	3128	49808	TCP	3128 → 49808 [PSH, ACK] Seq=4494 Ack=876 Win=31360 Len=4237 [TCP segment of a reassembled PDU]
192.168.1.53	192.168.1.…	3128	49808	TCP	3128 → 49808 [PSH, ACK] Seq=8731 Ack=876 Win=31360 Len=4096 [TCP segment of a reassembled PDU]
192.168.1.53	192.168.1.…	3128	49808	HTTP	HTTP/1.1 200 OK (PNG)
192.168.1.45	192.168.1.…	49808	3128	TCP	49808 → 3128 [ACK] Seq=876 Ack=8731 Win=2102272 Len=0
192.168.1.45	192.168.1.…	49808	3128	TCP	49808 → 3128 [ACK] Seq=876 Ack=16222 Win=2102272 Len=0
192.168.1.45	192.168.1.…	49808	3128	HTTP	GET http://top/favicon.ico HTTP/1.1
192.168.1.53	192.168.1.…	3128	49808	TCP	3128 → 49808 [PSH, ACK] Seq=16222 Ack=1261 Win=32512 Len=4239 [TCP segment of a reassembled P…
192.168.1.53	192.168.1.…	3128	49808	HTTP	HTTP/1.1 503 Service Unavailable (text/html)
192.168.1.45	192.168.1.…	49808	3128	TCP	49808 → 3128 [ACK] Seq=1261 Ack=20461 Win=2102272 Len=0
192.168.1.45	192.168.1.…	49808	3128	TCP	49808 → 3128 [ACK] Seq=1261 Ack=20629 Win=2102016 Len=0

```
Vary: Accept-Language\r\n
Content-Language: fr-fr\r\n
X-Cache: MISS from ProxyVotreNom\r\n
```

```
00f0  61 67 65 3a 20 66 72 2d  66 72 0d 0a 58 2d 43 61   age: fr- fr··X-Ca
0100  63 68 65 3a 20 4d 49 53  53 20 66 72 6f 6d 20 50   che: MIS S from P
0110  72 6f 78 79 56 6f 74 72  65 4e 6f 6d 0d 0a 58 2d   roxyVotr eNom··X-
0120  43 61 63 68 65 2d 4c 6f  6f 6b 75 70 3a 20 4d 49   Cache-Lo okup: MI
0130  53 53 20 66 72 6f 6d 20  50 72 6f 78 79 56 6f 74   SS from  ProxyVot
0140  72 65 4e 6f 6d 3a 33 31  32 38 0d 0a 56 69 61 3a   reNom:31 28··Via:
0150  20 31 2e 31 20 50 72 6f  78 79 56 6f 74 72 65 4e    1.1 Pro xyVotreN
0160  6f 6d 20 28 73 71 75 69  64 2f 33 2e 35 2e 32 37   om (squi d/3.5.27
0170  29 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   )··Conne ction: k
0180  65 65 70 2d 61 6c 69 76  65 0d 0a 0d 0a 0a 3c 68   eep-aliv e·····<h
0190  74 6d 6c 3e 3c 68 65 61  64 3e 0a 3c 6d 65 74 61   tml><hea d>·<meta
01a0  20 74 79 70 65 3d 22 63  6f 70 79 72 69 67 68 74    type="c opyright
01b0  22 20 63 6f 6e 74 65 6e  74 3d 22 22 3e 0a 3c 6d   " conten t="">·<m
01c0  65 74 61 20 68 74 74 70  2d 65 71 75 69 76 3d 22   eta http -equiv="
01d0  43 6f 6e 74 65 6e 74 2d  54 79 70 65 22 20 63 6f   Content- Type" co
01e0  6e 74 65 6e 74 3d 22 74  65 78 74 2f 68 74 6d 6c   ntent="t ext/html
```

votre serveur Proxy fonctionne correctement.
Faites une copie d'écran nommée « 6_wiresharkproxy.png » et déposez-la sur « celene ».

14. Filtrer les connexions au serveur « votreNom-proxy »

Sauvegardez votre fichier actuel « squid.conf » →

```
insacvl@votreNom-proxy:~$ sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.v1
[sudo] Mot de passe de insacvl :
```

Créez deux comptes utilisateurs sur la VM serveur « votreNom-proxy » :

- Un compte utilisateur portant **votre** nom de famille(exemple : szpieg).
- Un compte utilisateur portant **votre** prénom (exemple : martial ».

(**Vous mettrez votre nom de famille et votre prénom en minuscule sans accent ou espace!!!**).

Utilisez la commande « htpasswd »→

```
insacvl@votreNom-proxy:~$ htpasswd
La commande « htpasswd » n'a pas été trouvée, mais peut être installée avec :
sudo apt install apache2-utils
```

Remarque : cette commande fait partie du package « apache2-utils » donc installez-le !

Ci-contre la création de deux comptes →

```
insacvl@votreNom-proxy:~$ sudo htpasswd -c /etc/squid/passwords szpieg
New password:
Re-type new password:
Adding password for user szpieg
insacvl@votreNom-proxy:~$ sudo htpasswd  /etc/squid/passwords martial
New password:
Re-type new password:
Adding password for user martial
insacvl@votreNom-proxy:~$ cat /etc/squid/passwords
szpieg:$apr1$iLk7V2QK$MBXZNcQ4CWqRcuyebA9gz1
martial:$apr1$yZ0H1Gtl$W/KGg2cbmhUeBLqeACrnW/
```

Remarques :
L'option -c de la commande « htpasswd » veut dire « create » donc il faut la mettre que lors de la première utilisation sinon le fichier existant est vidé !!!
Comme mot de passe pour les deux comptes vous mettrez « azerty ».

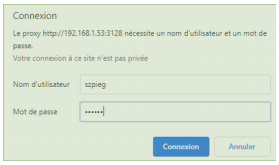
Faites un fichier nommé « 7_htpasswd.odt » ou « 7_htpasswd.docx » dans lequel vous expliquerez pourquoi les empreintes des mots de passe dans le fichier « /etc/squid/passwords » ne sont pas les mêmes alors que le mot de passe est « azerty » pour les deux comptes. Déposez « 7_htpasswd.odt » sur « celene ».

Vous trouverez sur « celene » un fichier nommé « 2020_2021_squid_with_auth.conf » dont vous pouvez vous inspirer pour réaliser votre fichier « /etc/squid/squid.conf ».
Attention : Dans le fichier « /etc/squid/squid.conf », le paramètre « visible_hostname » est à changer obligatoirement !

N'oubliez pas de redémarrer le service « Squid » et d'être patient cela prend un certain temps !

Retournez sur votre machine réelle, relancez « chrome » et allez sur un site INTERNET de votre choix.

Vous devriez obtenir ceci →



Faites une capture d'écran de cette fenêtre popup, appelez-la « 8_Authrequise.png » et déposez-la sur « celene ».

Connectez vous avec « votrenomdefamille », rappel mot de passe « azerty ».

Redémarrez « Chrome » et allez sur un autre site de votre choix.
Mettez dans la fenêtre de connexion pour le nom d'utilisateur « titi » mot de passe « azerty » et constatez le résultat.
Puis cliquez sur le bouton « Annuler » dans la fenêtre « POPUP » qui est réapparue.

Vous obtenez ceci →

Faites une copie d'écran **intégrale de la fenêtre popup** comme ci-contre, nommez-la « 8_errorsquid.png » et déposez-la sur « celene ».

15. Analyse de logs.

Allez sur la « VM » « VotreNom-Proxy » et dans un terminal tapez les lignes suivantes :

```
insacvl@votreNom-proxy:~$ sudo cat /var/log/squid/access.log |grep szpieg
1605006211.914     50 192.168.1.45 TCP_MISS/301 761 GET http://www.sncf.com/ szpieg HIER_DIRECT/158.58.182.192 text/html
1605006215.002   3082 192.168.1.45 TCP_TUNNEL/200 1321460 CONNECT www.sncf.com:443 szpieg HIER_DIRECT/158.58.182.192 -
1605006215.234   3148 192.168.1.45 TCP_TUNNEL/200 213451 CONNECT www.sncf.com:443 szpieg HIER_DIRECT/158.58.182.192 -
1605006215.268   3165 192.168.1.45 TCP_TUNNEL/200 334204 CONNECT www.sncf.com:443 szpieg HIER_DIRECT/158.58.182.192 -
1605006215.480   3380 192.168.1.45 TCP_TUNNEL/200 329778 CONNECT www.sncf.com:443 szpieg HIER_DIRECT/158.58.182.192 -
1605006220.640   8554 192.168.1.45 TCP_TUNNEL/200 53844 CONNECT www.sncf.com:443 szpieg HIER_DIRECT/158.58.182.192 -
1605006220.640   8553 192.168.1.45 TCP_TUNNEL/200 443227 CONNECT www.sncf.com:443 szpieg HIER_DIRECT/158.58.182.192 -
1605006220.641   5371 192.168.1.45 TCP_TUNNEL/200 5192 CONNECT www.sncf.com:443 szpieg HIER_DIRECT/158.58.182.192 -
insacvl@votreNom-proxy:~$ sudo cat /var/log/squid/access.log |grep titi
1605011590.511     12 192.168.1.45 TCP_DENIED/407 4441 GET http://yahoo.com/ titi HIER_NONE/- text/html
```

Faites une copie d'écran de votre résultat. Appelez-la « 9_logsquid.png » et déposez-la sur « celene ».