

TP 3 R401 Proxy :

1 Questions préliminaires

Exercice 1 : Rappelez quel est le rôle d'un proxy direct

Le proxy direct est comme une passerelle qui va relayer les informations allant de l'intérieur du réseau vers l'extérieur. Exemple avec des recherches internet qui vont être émises par un PC interne, relayée par le proxy et ainsi anonymisé les recherches sur internet. Propose des options permettant d'améliorer la qualité de service (Filtre, bloqueur de pub, etc...).

Exercice 2 : Quelle différence faites-vous avec le proxy inverse ?

La différence entre un serveur proxy direct et inverse sens des requêtes. Un proxy inverse se trouve du côté des serveurs web. Il anonymise les serveurs web en interceptant les requêtes clients et les basculant vers les serveurs. Propose des options supplémentaires pour améliorer la qualité de service (Équilibrage, filtre, cache, etc...).

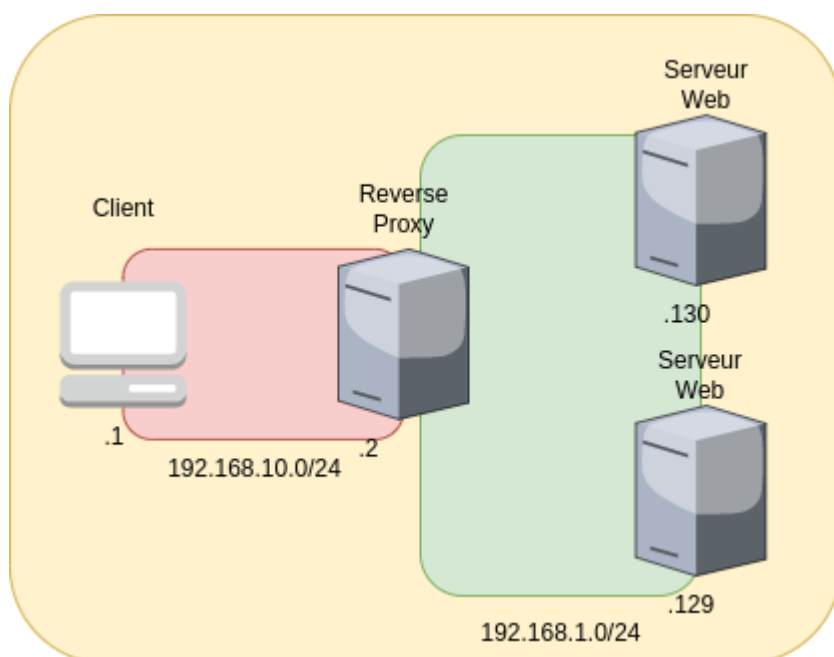
Exercice 3 : Citez quelques exemples de solutions permettant de réaliser ces fonctions.

Proxy direct : Squid, WinGate, etc... Proxy inverse : Nginx, Apache HTTP, etc...

2 Proxy direct

Exercice 4-5

Plan d'adressage de mon réseau :



Installation de apache2 sur le serveur web et de squid (Je passe les photos de l'installation étant simplement un `apt install`). Puis je configure le fichier de squid comme suit :

J'ai mis en source la plage d'IP du : poste client/proxy et proxy/serveurWeb en faisant un `acl localnet10 src 192.168.10.0/24` et `acl localnet1 src 192.168.1.0/24`. Et ajouter la ligne `http_access deny !localnet1` cette commande refuse tout autre ip n'étant pas 192.168.1.X.

Exercice 6

J'utilise les règles de routage vu au TP 2 pour que les deux réseaux soit connecté :

Proxy :

```
sudo echo 1 > /proc/sys/net/ipv4/ip_forward iptables -t nat -A POSTROUTING  
-s 192.168.1.0/24 -o ens33 -j MASQUERADE
```

PC client :

```
ip a add 192.168.1.1/24 dev ens33 && ip r add default via 192.168.1.130 dev  
ens33
```

Exercice 7

Voir exercice 4-5 ou j'ai configuré l'option de capter le trafic du réseau local précis. Exemple ici ou ma machine client est en 192.168.10.X/24 donc la connection est refusé:



The proxy server is refusing connections

Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

Try Again

Les lignes refresh pattern permet de gérer les options liées au cache des pages. Par exemple je pourrais ajouter cette commande (Je me suis inspiré de sur un site) : `refresh_pattern -i . (gif|png|jpg|jpeg|ico|bmp|tiff?)$ 600 100% 600 override-expire override-lastmod reload-into-ims`

Ici je sauvegarde les gif, png, etc... Pendant 10 minute(600 sec).

Exercice 8

nftable :

```
sudo nft add table filter
sudo nft add chain filter input { type filter hook input priority 0 \; }
sudo nft add rule filter input ip daddr 192.168.1.0/24 tcp dport 80
redirect to :3128
#Redirige tout le traffique tcp port 80 vers le proxy port 3128.

sudo nft add rule filter input ip protocol tcp counter drop
#Bloquent tout le trafic qui ne respecte pas les règles précédentes
```

Exercice 9

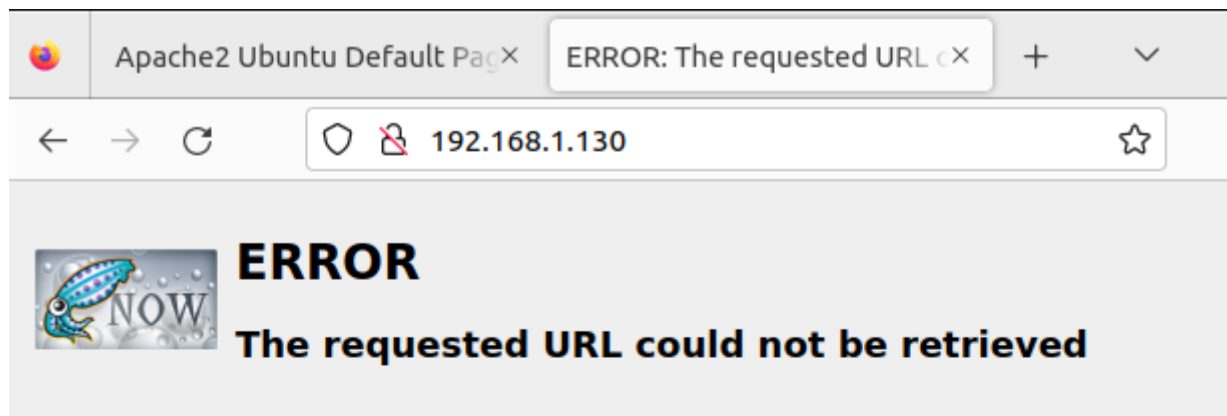
Commande effectuée pour bloquer un site :

```
#Pour bloquer une IP :
acl BlockedHost src 192.168.1.130

#TIPS : Pour bloquer un lien Camarade : acl camarade dstdomain
.camarade.com
http_access deny BlockedHost

sudo systemctl restart squid
#Redémarrer pour actualiser la conf
```

```
acl BlockedHost dst 192.168.1.130
acl localnet10 src 192.168.10.0/24
acl localnet1 src 192.168.1.0/24
#
acl SSL_ports port 443
acl Safe_ports port 80
acl Safe_ports port 21
acl Safe_ports port 443
acl Safe_ports port 70
acl Safe_ports port 210
acl Safe_ports port 1025-65535
acl Safe_ports port 280
acl Safe_ports port 488
acl Safe_ports port 591
acl Safe_ports port 777
#
http_access deny BlockedHost
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
#http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
#
http_port 3128
#
coredump_dir /var/spool/squid
#
refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:      1440      0%        1440
refresh_pattern -i (/cgi-bin/|\?) 0        0%         0
refresh_pattern \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern \/(Release(|\.gpg)$ 0 0% 0 refresh-ims
refresh_pattern \/(InRelease$ 0 0% 0 refresh-ims
refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern .              0        20%      4320
```



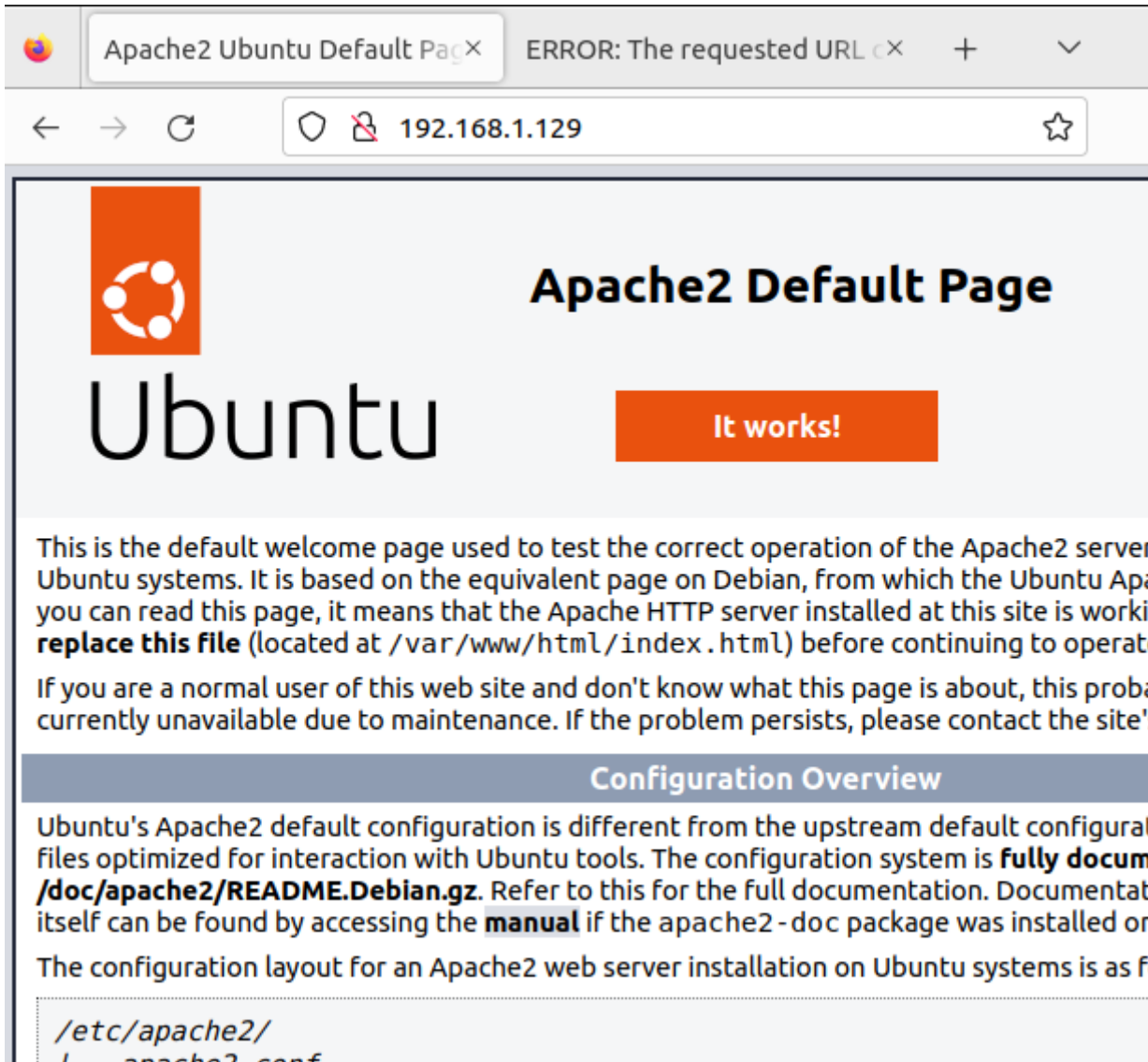
The following error was encountered while trying to retrieve the URL: <http://192.168.1.130/>

Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your provider if you feel this is incorrect.

Your cache administrator is [webmaster](#).

Generated Sun, 02 Apr 2023 11:00:36 GMT by client1 (squid/5.6)



Comme vu sur les photos précédentes l'accès est bien bloqué au serveur 192.168.1.130, mais toujours possible au site 192.168.1.129.

Exercice 10 :

Le flux TCP passe bien par le proxy de ce que je comprends sur Wireshark :

265	20.085531430	192.168.10.129	192.168.10.1	TCP	78 51454 → 53 [SYN] Seq=0 Win=64240 Len=0 MS
266	20.085551336	192.168.10.1	192.168.10.129	TCP	54 53 → 51454 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
267	20.085667702	192.168.10.129	192.168.10.1	TCP	78 51458 → 53 [SYN] Seq=0 Win=64240 Len=0 MS
268	20.085679995	192.168.10.1	192.168.10.129	TCP	54 53 → 51458 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
269	20.085803904	192.168.10.129	192.168.10.1	TCP	78 51470 → 53 [SYN] Seq=0 Win=64240 Len=0 MS
270	20.085815499	192.168.10.1	192.168.10.129	TCP	54 53 → 51470 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
271	20.085916707	192.168.10.129	192.168.10.1	DNS	86 Standard query 0x75dd A www.google.com.localdomain
272	20.085978732	192.168.10.129	192.168.10.1	DNS	86 Standard query 0x2419 AAAA www.google.com.localdomain
273	20.086033492	192.168.10.129	192.168.10.1	DNS	74 Standard query 0xbfa5 A www.google.com.localdomain
274	20.249235403	192.168.10.130	192.168.10.1	DNS	86 Standard query 0x8a58 A ntp.ubuntu.com.localdomain
275	20.249265018	192.168.10.1	192.168.10.130	ICMP	114 Destination unreachable (Port unreachable)
276	20.249391721	192.168.10.130	192.168.10.1	DNS	86 Standard query 0x9212 AAAA ntp.ubuntu.com.localdomain
277	20.249403525	192.168.10.1	192.168.10.130	ICMP	114 Destination unreachable (Port unreachable)
278	20.250264183	192.168.10.130	192.168.10.1	TCP	78 53318 → 53 [SYN] Seq=0 Win=64240 Len=0 MS
279	20.250279060	192.168.10.1	192.168.10.130	TCP	54 53 → 53318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
280	20.250409116	192.168.10.130	192.168.10.1	TCP	78 53326 → 53 [SYN] Seq=0 Win=64240 Len=0 MS
281	20.250421549	192.168.10.1	192.168.10.130	TCP	54 53 → 53326 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
282	20.250564107	192.168.10.130	192.168.10.1	TCP	78 53338 → 53 [SYN] Seq=0 Win=64240 Len=0 MS
283	20.250576121	192.168.10.1	192.168.10.130	TCP	54 53 → 53338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
284	20.250693883	192.168.10.130	192.168.10.1	DNS	74 Standard query 0x4a31 AAAA ntp.ubuntu.com.localdomain
285	20.250719657	192.168.10.1	192.168.10.130	ICMP	102 Destination unreachable (Port unreachable)
286	20.250840283	192.168.10.130	192.168.10.1	DNS	74 Standard query 0x29e1 A ntp.ubuntu.com.localdomain
287	20.250853275	192.168.10.1	192.168.10.130	ICMP	102 Destination unreachable (Port unreachable)
288	20.251134549	192.168.10.130	192.168.10.1	DNS	74 Standard query 0x7e75 A ntp.ubuntu.com.localdomain
289	20.251147960	192.168.10.1	192.168.10.130	ICMP	102 Destination unreachable (Port unreachable)
290	20.251317898	192.168.10.130	192.168.10.1	DNS	74 Standard query 0x83b9 AAAA ntp.ubuntu.com.localdomain

On aperçoit dans les logs les ip des accès au proxy et aussi les logs du proxy.

```
1680435494.728    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435494.892    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435495.054    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435495.223    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435807.047    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435811.288    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435811.874    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435812.566    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435813.492    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435813.682    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435864.831  20365 192.168.10.129 TCP_MISS/500 4520 GET http://detectportal.firefox.com/success.t
xt? - HIER_NONE/- text/html
1680435864.831  20366 192.168.10.129 TCP_MISS/500 4520 GET http://detectportal.firefox.com/success.t
xt? - HIER_NONE/- text/html
1680435876.079  31490 192.168.10.129 NONE_NONE/500 0 CONNECT push.services.mozilla.com:443 - HIER_NO
NE/- -
1680435881.871    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435882.007    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435882.307    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435882.524    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
1680435882.706    0 192.168.10.129 TCP_INM_HIT/304 268 GET http://192.168.1.129/ - HIER_NONE/- tex
t/html
root@client1:/etc/squid# ~_
```

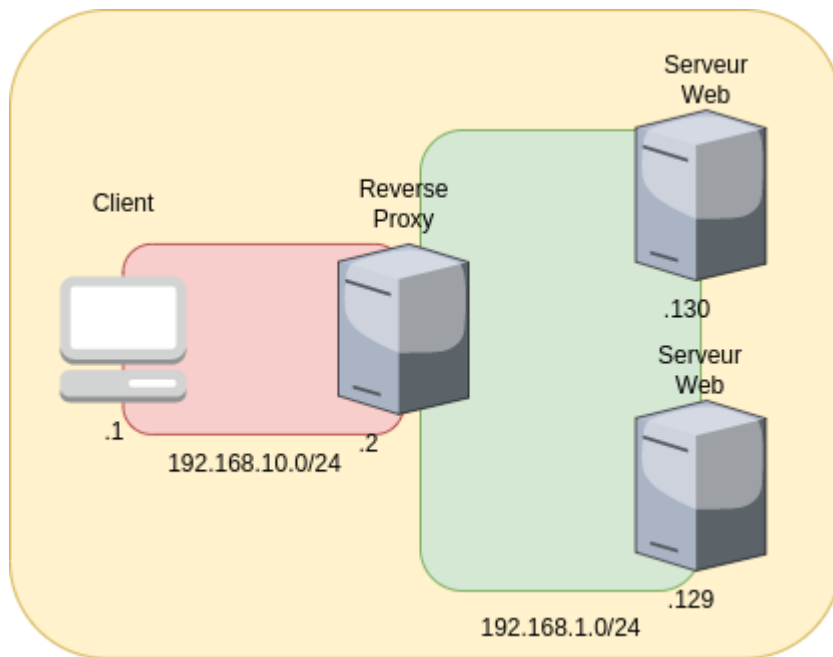
Exercice 11 :

Il peut y avoir des ralentissements, par exemple si la machine support n'est pas assez performante. Des erreurs de configuration ou encore si le proxy perd la connexion tout le réseau est impactée.

```
#Lignes mofifiées dans le fichier de conf squid pour parvenir à avoir un
résultat cohérent :
acl BlockedHost dst 192.168.1.130
acl localnet src 192.168.1.0/24
http_access deny BlockedHost
http_acces allow localnet
refresh_pattern -i (.gif|png|jpg|jpeg|ico|bmp|tiff?)$ 600 100% 600
override-expire override-lastmod reload-into-ims
```

3 Proxy reverse

Exercice 12 :



Exercice 13-14:

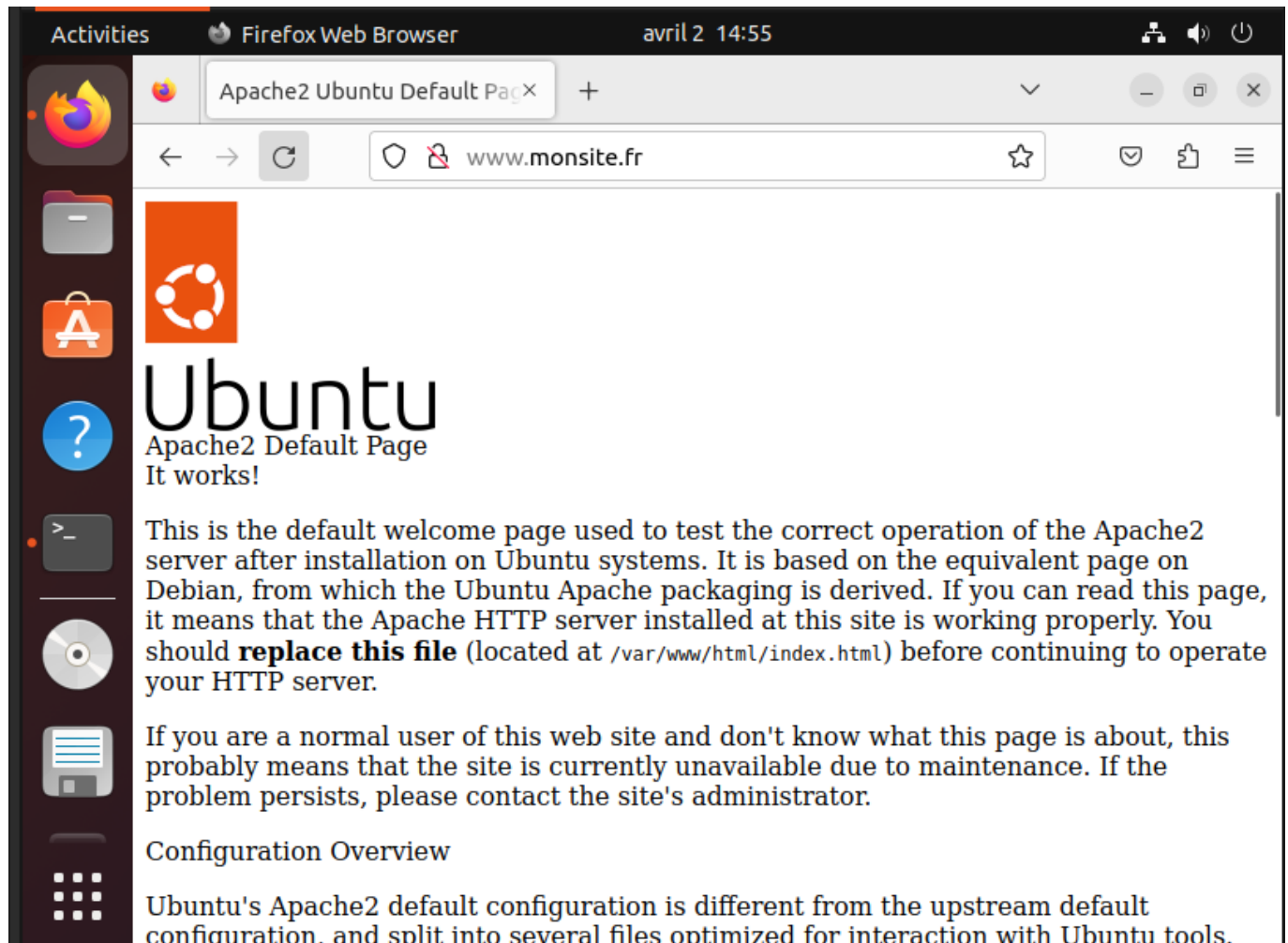
Installation effectuer via `apt install`.

Exercice 15-16 :

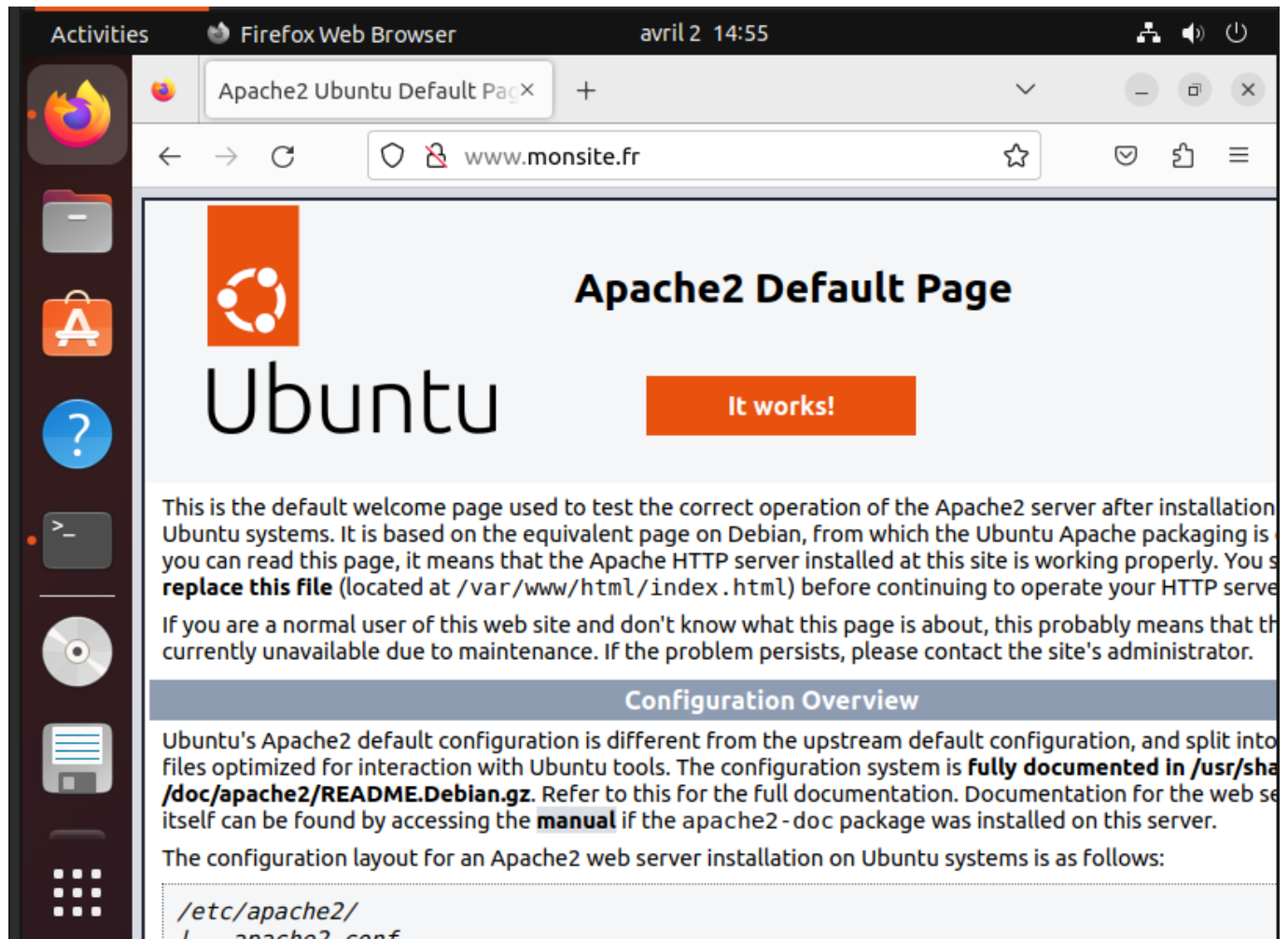
Voilà le résultat avec configuration activé, il suffit d'un F5 (refresh) pour alterner entre les deux sites web :

Côté client :

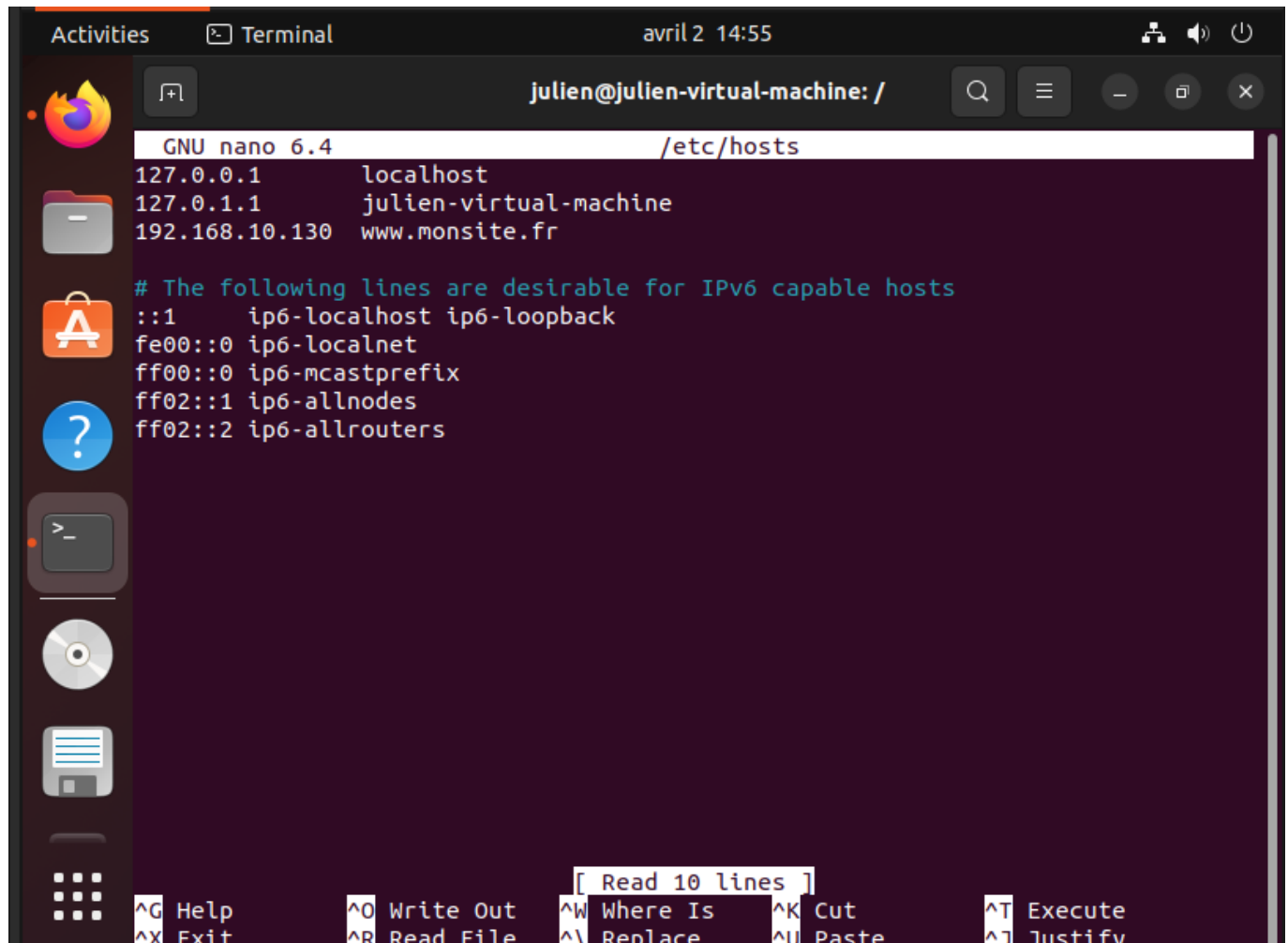
Site modifier 192.168.1.129 :



Site non-modifié 192.168.1.130 :



Configuration du fichier hosts :



The screenshot shows a terminal window titled 'julien@julien-virtual-machine: /' with a timestamp of 'avril 2 14:55'. The terminal is running the GNU nano 6.4 editor, editing the file /etc/hosts. The content of the file is as follows:

```
127.0.0.1    localhost
127.0.1.1    julien-virtual-machine
192.168.10.130 www.monsite.fr

# 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
```

At the bottom of the terminal, a status bar displays various keyboard shortcuts for nano editor operations:

Shortcut	Operation
^G	Help
^O	Write Out
^W	Where Is
^K	Cut
^T	Execute
^X	Exit
^R	Read File
^_	Replace
^U	Paste
^J	Justify

Côté proxy :

J'ai créé un fichier `load-balancing.conf` dans `/etc/nginx/conf.d/` est inséré la configuration :

[illegible]

```
# partie de la configuration de nginx
upstream backend {
    server 192.168.1.129 weight=1;
    server 192.168.1.130 weight=1;
}
server {
    listen 80;
    server_name www.monsite.fr monsite.fr;
    location / {
        proxy_pass http://backend;
    }
}
```