M4210-TP4-Proxy - INFRASTRUCTURES DE SECURITE

Samedi 22 février 2019

Amine ABDOUL-AZID

Florian BAKRY

**PRÉPARATION :**

1. Le PC du LAN a besoin de faire une résolution de noms même s’il passe par le proxy.
2. Le firewall doit être configurer en statefull pour obliger à passer par le proxy ou il doit bloquer les autres réseaux.
3. Le LAN a besoin d’une passerelle par défaut pour joindre le proxy car le traceroute affiche qu’il passe d’abord par le routeur.

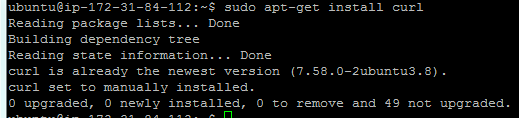
sudo apt-get update -y

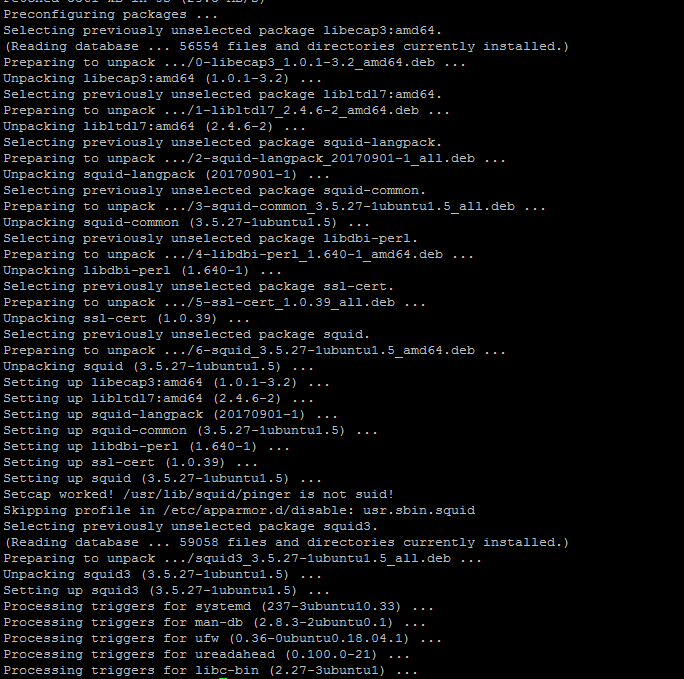
sudo apt-get install -y curl

sudo apt-get install -y squid3

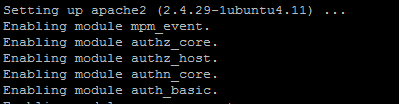
sudo apt-get install -y apache2-utils

sudo apt-get install -y apache2









sudo ifdown eth0

sudo ifup eth0

./fwcheck.sh

./vhost.sh

sudo rm /var/www/html/index.html && sudo echo superman > /var/www/html/kikoulol.exe

sudo gedit /etc/hosts

[www.kaceboof.com](http://www.kaceboof.com) 198.51.100.42

www1.spachnat.com 198.51.100.42

www2.spachnat.com 198.51.100.42

tendir.com 198.51.100.42

[www.lorieforever.fr](http://www.lorieforever.fr) 198.51.100.42

[www.gogleo.fr](http://www.gogleo.fr) 198.51.100.42

[www.delichoc.fr](http://www.delichoc.fr) 198.51.100.42

delichoc-my.shorepaint.com 198.51.100.42

52.91.209.54



sudo cp /etc/squid/squid.conf /home/etudiant/

sudo echo http\_port 3128 >> /etc/squid/squid.conf

sudo systemctl restart squid && sudo gedit /etc/squid/squid.conf

navig : 192.0.2.2 3128

#R1

acl mes\_reseaux src 192.0.2.0/24

#R2

acl acces\_spachnat dstdomain www1.spachnat.com

http\_access deny acces\_spachnat

acl acces\_spachnat2 dstdomain www2.spachnat.com

http\_access deny acces\_spachnat2

acl acces\_kaceboof dstdomain www.kaceboof.fr

http\_access deny acces\_kaceboof

acl acces\_tendir dstdomain tendir.com

http\_access deny acces\_tendir

acl acces\_lorie dstdomain www.lorieforever.fr

http\_access deny acces\_lorie

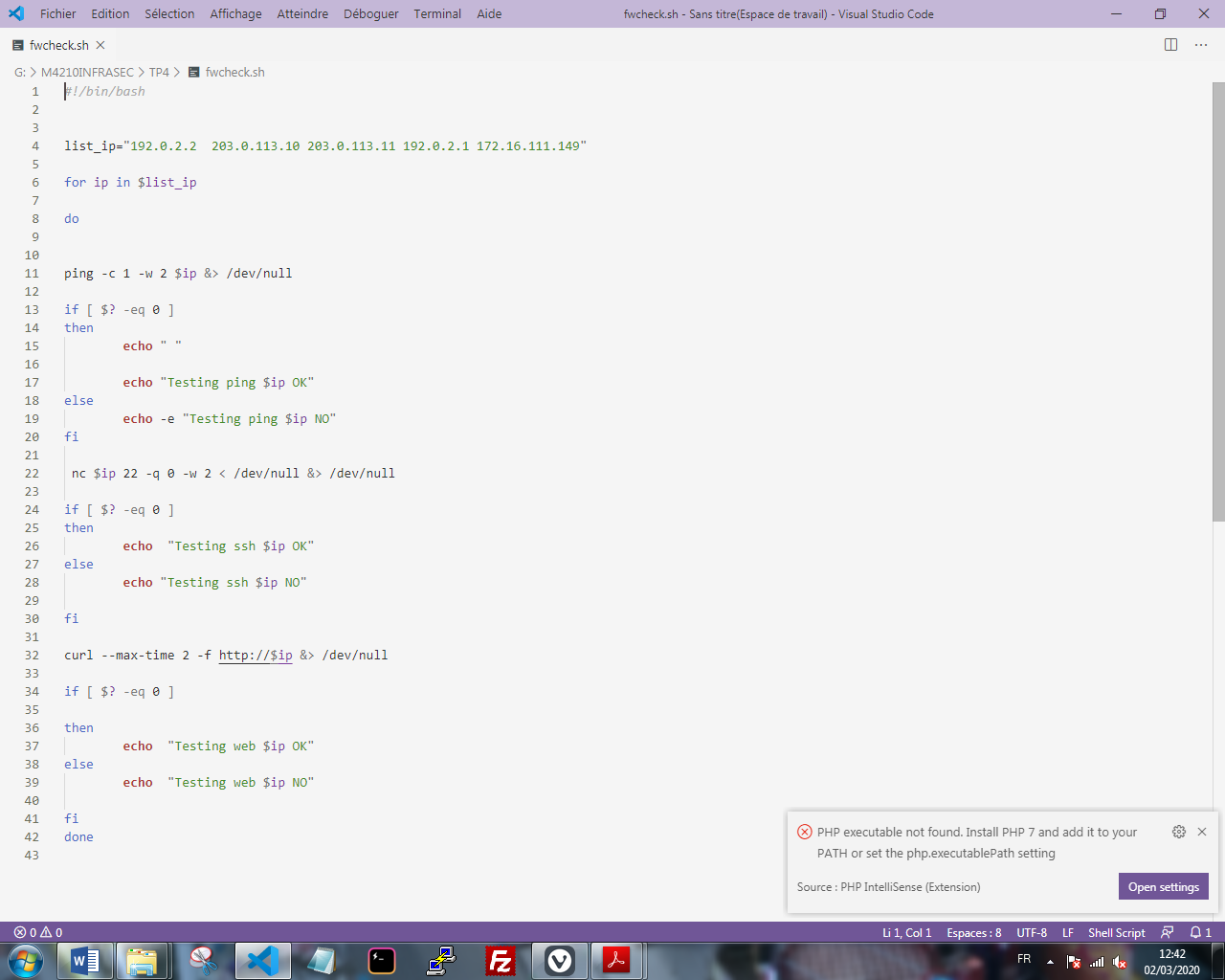
#R3

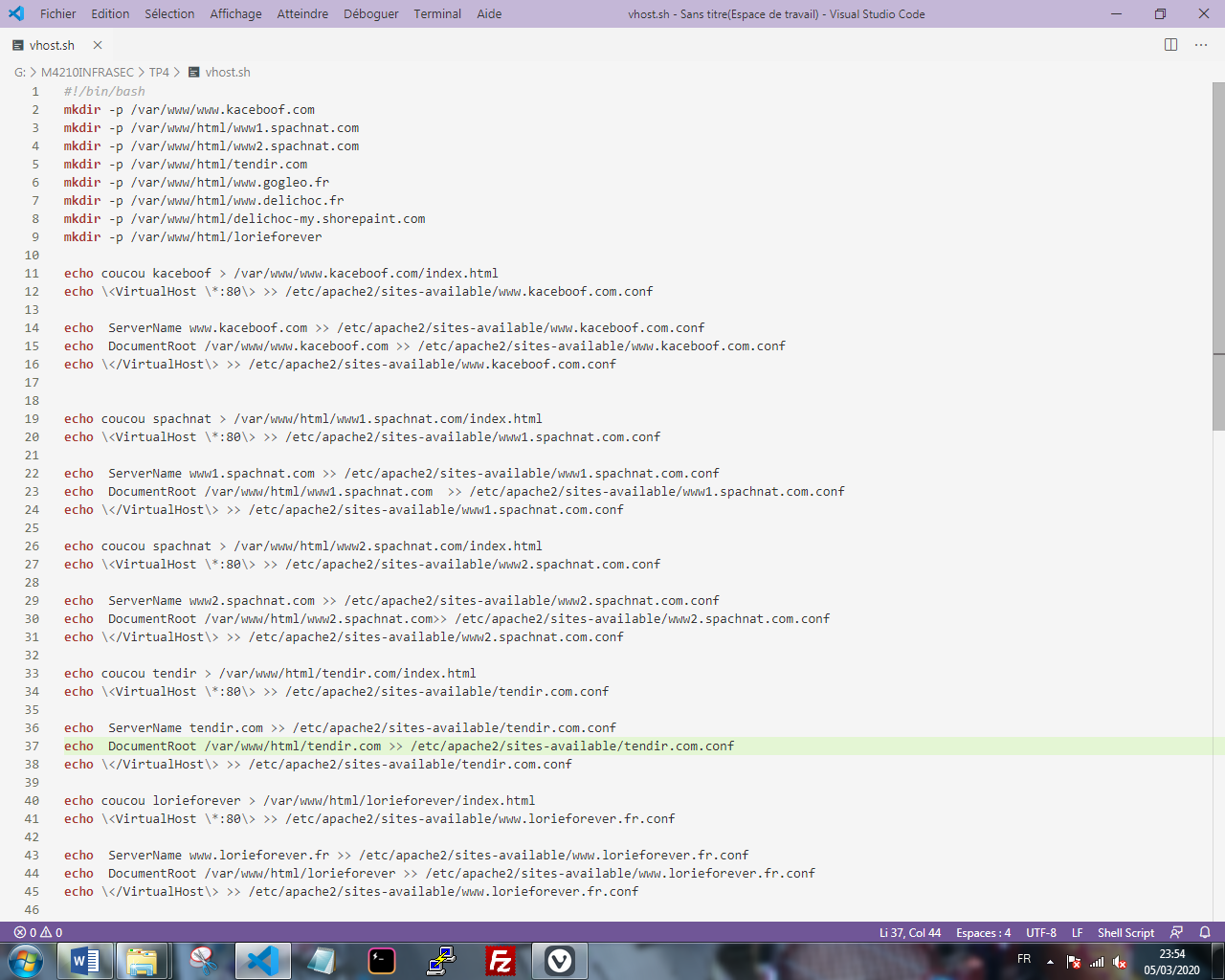
acl fichier\_exe urlpath\_regex \.exe(\?.\*)?$

http\_access deny fichier\_exe

sudo systemctl status squid.service && sudo gedit /var/log/squid/access.log && sudo gedit /var/log/squid/cache.log

sudo chmod u+x \*.sh && sudo ./proxycheck.sh





**Synthèse 1 :**

Pour commencer nous avons tout d’abord vu que la date était à la bonne heure puis installé les paquets, on a configuré en statique les adresses IP, on a édité le fichier Host sur le proxy. Enfin on a vérifié que les pages s’affichent. On a copié le fichier de configuration. Les sites étaient bloqués sur le LAN. On a bloqué explicitement des sites et le téléchargement des exécutables.

#R4

acl pausemidi time 12 :00-14:00

acl acces\_spachnat dstdomain www1.spachnat.com

http\_access access acces\_spachnat

acl acces\_spachnat2 dstdomain www2.spachnat.com

http\_access access acces\_spachnat2

acl acces\_kaceboof dstdomain www.kaceboof.fr

http\_access access acces\_kaceboof

acl acces\_tendir dstdomain tendir.com

http\_access access acces\_tendir

acl acces\_lorie dstdomain www.lorieforever.fr

http\_access access acces\_lorie

#R5

acl my\_reseaux src 192.0.2.50

acl acces\_spachnat dstdomain www1.spachnat.com

http\_access access acces\_spachnat

acl acces\_spachnat2 dstdomain www2.spachnat.com

http\_access access acces\_spachnat2

acl acces\_kaceboof dstdomain www.kaceboof.fr

http\_access access acces\_kaceboof

acl acces\_tendir dstdomain tendir.com

http\_access access acces\_tendir

acl acces\_lorie dstdomain www.lorieforever.fr

http\_access access acces\_lorie

acl fichier\_exe urlpath\_regex \.exe(\?.\*)?$

http\_access access fichier\_exe

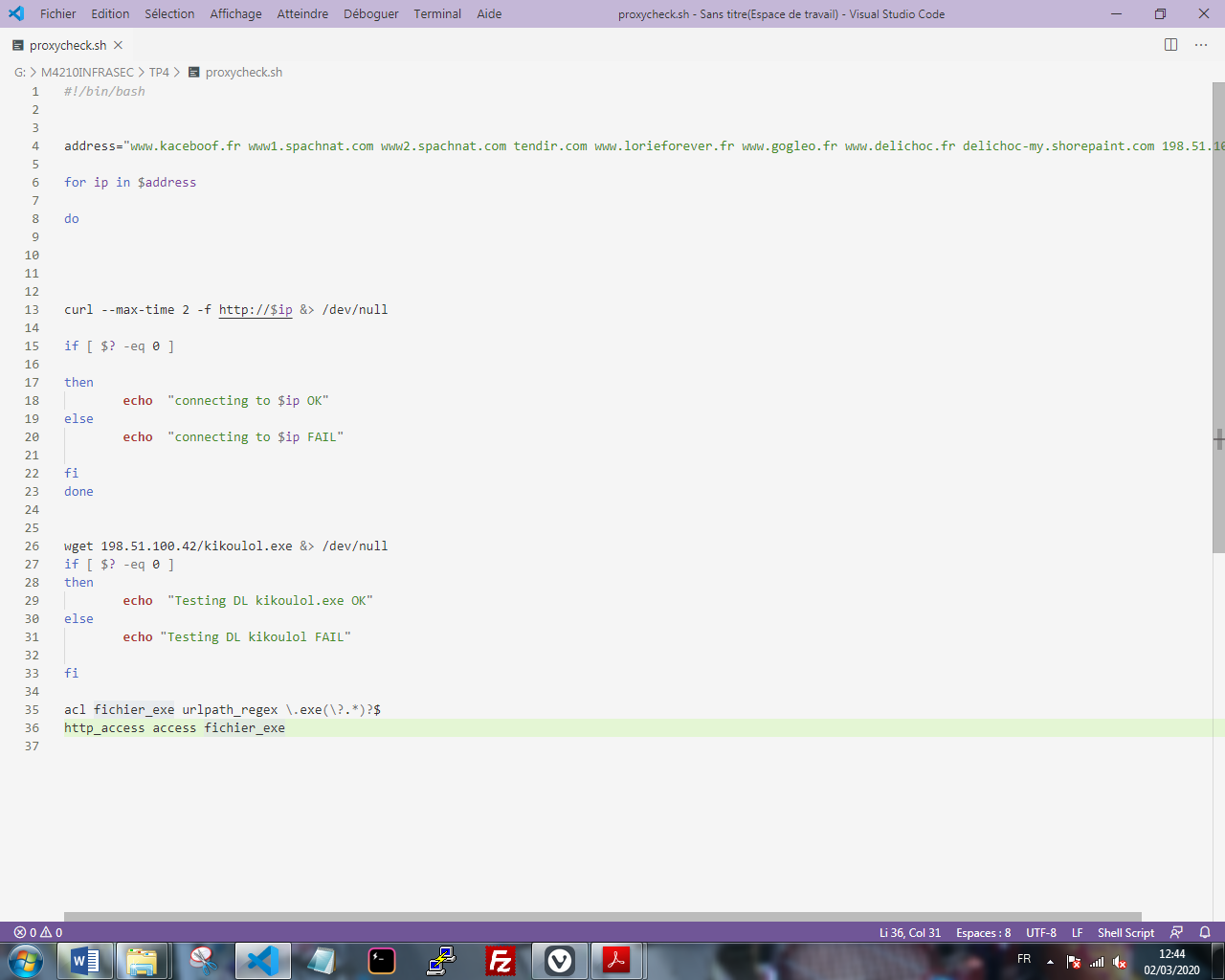
#R6

acl reseaux src 192.0.2.42

acl fichier\_exe urlpath\_regex \.exe(\?.\*)?$

http\_access access fichier\_exe

sudo ./proxycheck.sh



ip a flush dev eth0

ip a add 192.0.2.50/42 dev eth0

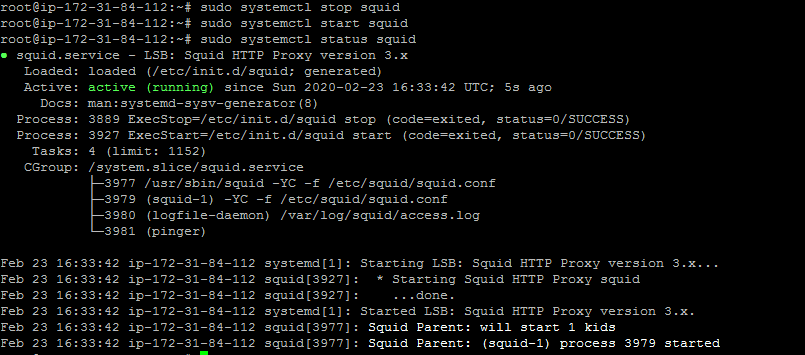
ip a del 192.0.2.50/42 dev eth0

ip a add 192.0.2.42/42 dev eth0

ip a del 192.0.2.42/42 dev eth0

sudo ifdown eth0 && sudo ifup eth0 && sudo gedit /etc/network/interfaces

ip a add 192.0.2.100/42 dev eth0



**Synthèse 2 :**

On a changé l’heure à 13H00. On a ajouté une adresse éphémère on a ajouté des règles Proxy selon les adresses IP. On a ajouté une règle en fonction d’une période horaire, on a autorisé le téléchargement de fichiers exécutable.

#R7

acl the\_reseaux src 198.51.100.0/24

cd /etc/squid/

htpasswd -m users.txt white < vitrygtr

/usr/lib/squid3/basic\_ncsa\_auth users.txt < white vitrygtr

htpasswd -m users.txt pinkman < vitrygtr

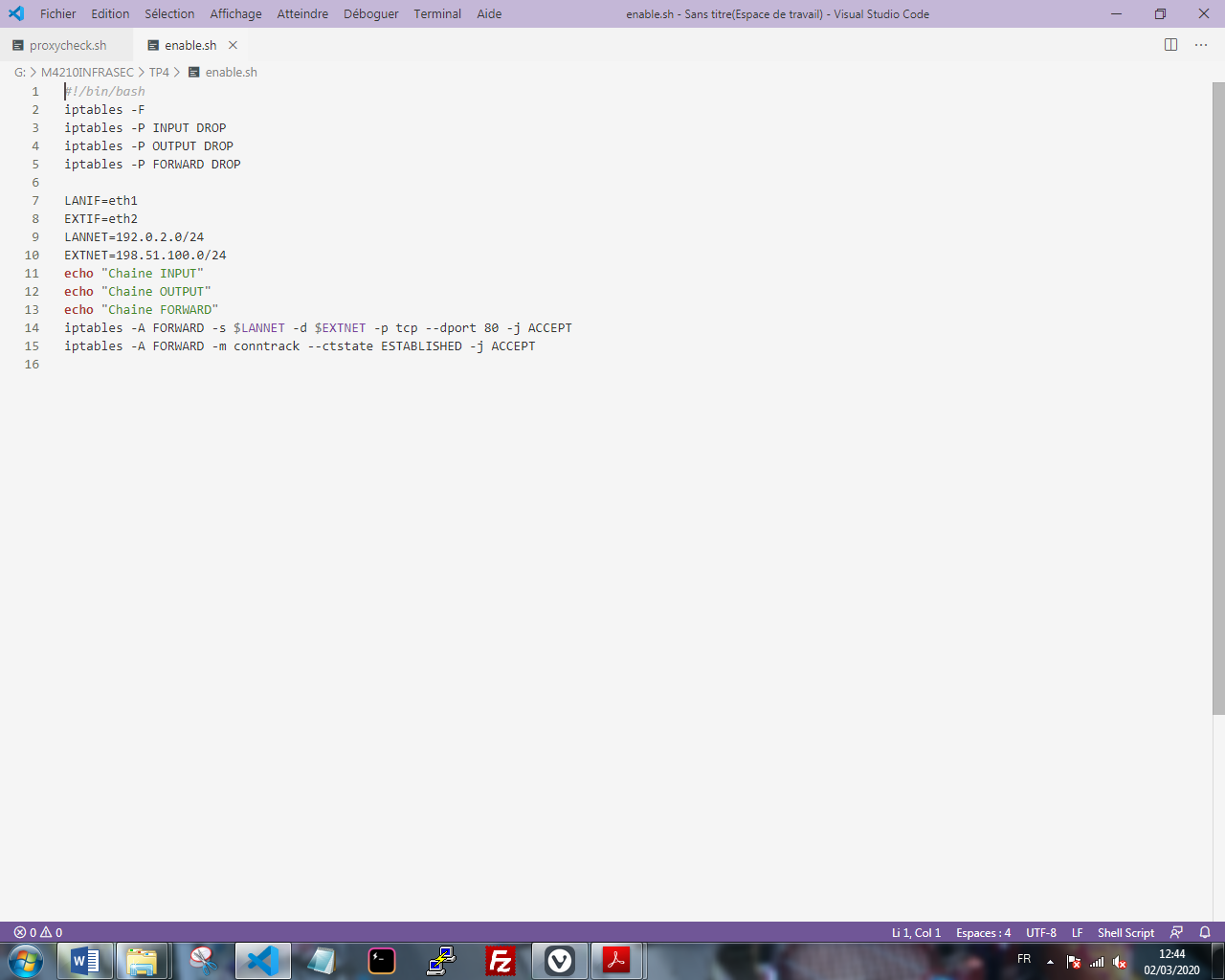
/usr/lib/squid3/basic\_ncsa\_auth users.txt < pinkman vitrygtr

auth\_param basic program /usr/lib/squid3/basic\_ncsa\_auth /etc/squid/users.txt

acl authentif\_necessaire proxy\_auth REQUIRED

#FW

./enable.sh



**Synthèse 3 :**

Les utilisateurs d’un autre réseau que le LAN doivent s'authentifier s'ils utilisent le proxy.

On a utilisé une authentification NCSA .On a ajouté une règle avec un ACL pour permettre l’authentification. On a configuré le firewall pour que seul le proxy soit habilité à se connecter au Serveur APACHE.



Woo hoo ! Adieu ! On est génial n’est-ce pas !!

**Annexes :**