MISE EN PLACE DU SERVEUR WEB SECURISEE

Apache2, modules apache, fail2ban, php, mysql

Le serveur HTTP Apache2 a une bonne réputation en matière de sécurité. Mais il est inévitable d'ajuster votre serveur web à quelques recommandations cités dans ce guide afin de répondre aux besoins à l'abri des menaces web et en garantissant une performance élevé. Donc ce guide décrit les étapes d'installation et de configuration d'apache2 et ses modules de sécurité ainsi que la configuration de PHP et de mysql, en citant à la fin quelques méthodes de supervision du serveur apache.

Agence Nationale de la Sécurité Informatique

Gestion de document

Auteur	Version	Date	Modification apportée
B.H	1.0	27/05/2011	Première version

Document Publique

Document Interne

PLAN

1. Pré requis

Deux disques durs en mirorring hardware, le cas échéant software ou LVM.

2. Installation système

2.1. Partitionnement

Au cours d'installation de votre système d'exploitation, il est recommandé de bien partitionner votre disque, comme suit, afin de le configurer avec une performance maximale.

/	14 Go
/ boot	1 Go
/tmp	14 Go
/var	50 Go
Swap	16 Go
Le reste en LVM (*)	

(*) Le reste servira comme extension des autres volumes logiques en cas de besoin.

2.2. Installation

Poursuivre l'installation avec une installation minimale des services.

2.3. Tunning système

- Désinstallation des protocoles réseaux inutiles :

Désactiver IPV6 et ceci en modifiant /etc/modprobe.d/aliases.conf

- Elimination des services inutiles :

Utiliser pour cela les commandes #netstat –anp|grep -i liste Et #dpkg –l

3. POST INSTALLATION

Pour un serveur web avec mutualisation changez apache2-mpm-prefork avec apache2-mpm-itk.

Dans notre cas on a :

#apt-get install ssh #apt-get install iproute #apt-get install libapache2-mod-php5 apache2 #apt-get install libapache2-mod-bw #apt-get install libapache2-mod-evasive #apt-get install mysql-server php5-mysql #apt-get install liblua5.1-0 libapache2-mod-security2 #apt-get install fail2ban #apt-get install aide

```
#apt-get install clamav

#apt-get install awstats

#apt-get install apachetop
```

3.1. Partage de mémoires

Le serveur contient 1 Go de RAM qu'on va partager comme suit:

Le système d'exploitation	256 Mo
La base de données « mysql »	256 Mo
Le reste pour apache	512 Mo

3.2. Tunning Mysql

- En utilisant l'interpréteur mysql déterminer les valeurs des variables « table_open_cache » et « key_buffer_size », à cet effet utiliser (show variables like '%motif%';).
- Changer les variables suivantes dans /etc/mysql/my.cnf

```
table_open_cache 256

key_buffer_size 64M

query_cache_size 32M

sort_buffer_size 4M

read_buffer_size 1M
```

- puis redémarrer mysql (/etc/init.d/mysql restart) revérifier les variables.
- Et pour suivre les requêtes langues plus que 10s on ajoute :

```
log_slow_queries       = /var/log/mysql/mysql-slow.log

long_query_time = 10
```

- L'administration peut être banalisé par mysql-workbench et l'accès au serveur se fait par tunnel ssh 3306➔localhost : 3306 en utilisant putty

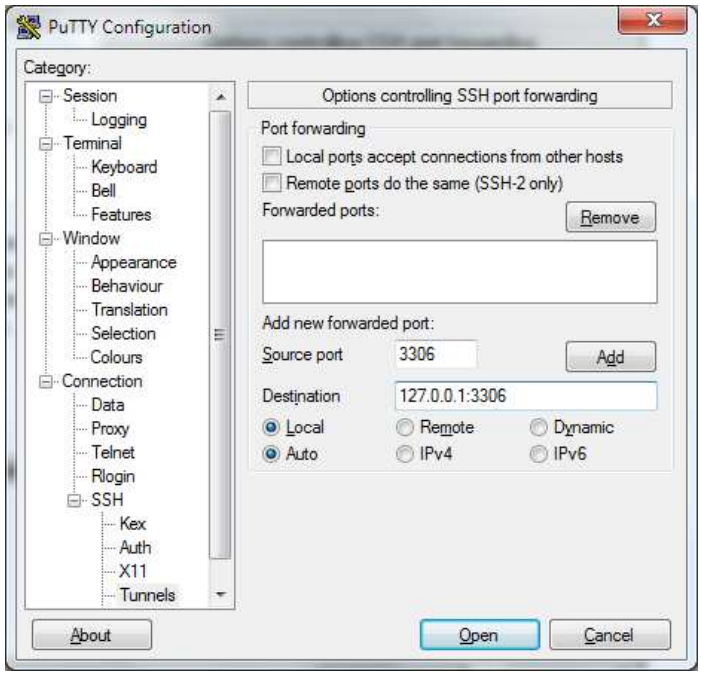

Fig1. Configuration de Putty

- Pour cela ajouter un utilisateur nommé « WebRO » qui a les droits « select » sur la base de données qui servira pour les pages web en consultation seulement.
- Et un utilisateur nommé « WebRW » qui a les droit « select, update, insert et delete » qui servira pour les pages web qui modifient la base.

3.3. Configuration d'apache

- On va réserver, comme dans le tableau ci-dessus, « 512 Go » de RAM pour apache. Sachant que chaque processus serveur consomme vers « 8 Mo » (somme de RES-SHR de la commande top –u www-data) on a donc 64. Mais sachez que cela nécessite un étalonnage en suivant le serveur par top –u www-data et top –u mysql.
- Éditer le fichier /etc/apache2/envvars

```
export APACHE_RUN_USER=www-data

export APACHE_RUN_GROUP=www-data

export APACHE_PID_FILE=/var/run/apache2.pid
```

- Placer l'icône qui présente « serveur.tn » dans /var/www/favicon.ico
- Editer le fichier /etc/apache2/apache2.conf et analyser les paramètres suivants:

```
ServerRoot "/etc/apache2"

LockFile /var/lock/apache2/accept.lock

PidFile ${APACHE_PID_FILE}

Timeout 30

KeepAlive On

MaxKeepAliveRequests 50

KeepAliveTimeout 15

<IfModule mpm_prefork_module>

  #nombre maximal de processus serveurs

   ServerLimit                64

   StartServers         8

   MinSpareServers      8

   MaxSpareServers      16

  #nombre maximal de clients

   MaxClients         64

   Max request par processus serveur

   MaxRequestsPerChild   1000

</IfModule>

User ${APACHE_RUN_USER}

Group ${APACHE_RUN_GROUP}

AccessFileName .htaccess

<Files ~ "^\.ht">
```

```
    Order allow,deny

    Deny from all

</Files>

DefaultType text/plain

HostnameLookups Off

ErrorLog /var/log/apache2/error.log

LogLevel warn

Include /etc/apache2/mods-enabled/*.load

Include /etc/apache2/mods-enabled/*.conf

Include /etc/apache2/httpd.conf

Include /etc/apache2/ports.conf

LogFormat "%v:%p %h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

LogFormat "%h %l %u %t \"%r\" %>s %b" common

LogFormat "%{Referer}i -> %U" referer

LogFormat "%{User-agent}i" agent

CustomLog /var/log/apache2/other_vhosts_access.log vhost_combined

    ErrorDocument 400 "500"

    ErrorDocument 401 "500"

    ErrorDocument 403 "500"

    ErrorDocument 404 "500"

    ErrorDocument 405 "500"
```

```
    ErrorDocument 408 "500"

    ErrorDocument 410 "500"

    ErrorDocument 411 "500"

    ErrorDocument 412 "500"

    ErrorDocument 413 "500"

    ErrorDocument 414 "500"

    ErrorDocument 415 "500"

    ErrorDocument 500 "500"

    ErrorDocument 501 "500"

    ErrorDocument 502 "500"

    ErrorDocument 503 "500"

    ErrorDocument 506 "500"

Include /etc/apache2/conf.d/

#disable etag qui donne les infos temps pour les caches

Header unset ETag

FileETag None

ServerName www.serveur.tn

Include /etc/apache2/sites-enabled/
```

- Ajouter au fichier /etc/hosts une entrée vers servername :
- A.B.C.D www.serveur.tn
- Le fichier /etc/apache2/conf.d/security

```
<Directory />
```

```
        AllowOverride None

        Order Deny,Allow

        Deny from all

</Directory>

ServerTokens Prod

ServerSignature Off

TraceEnable Off
```

- Supprimer les modules inutiles : autoindex et status

```
a2dismod autoindex

a2dismod status
```

- Ajouter les types de fichier text/css appliaction/javascript au module deflat

```
# vi /etc/apache2/mods-available/deflate.conf

-----------------------------------------------------------------------

<IfModule mod_deflate.c>

 AddOutputFilterByType DEFLATE text/html text/plain text/xml text/css application/javascript

</IfModule>
```

❖ Paramétrages de status.conf :

- Si c'est décidé d'utiliser le module « status » qu'on a supprimé alors limité l'accès au server-status pour l'adresse IP de l'administrateur

```
# vi /etc/apache2/mods-available/status.conf

-----------------------------------------------------------------------

<IfModule mod_status.c>
```

```
<Location /server-status>
    SetHandler server-status
    Order deny,allow
    Deny from all
    Allow from localhost ip6-localhost 172.16.7.101 193.95.69.210
</Location>
ExtendedStatus On
</IfModule>
```

```
# a2enmod status
```

❖ Paramétrage du mod-evasive :

- On va prendre comme configuration que si une adresse IP accède plus de 5 fois à la même page en 3s, ou à plus de 30 requêtes sur tout le site en 1s, il sera banni (erreur HTTP 403) pendant 60s. Une notification sera alors envoyée à syslog.

```
# vi /etc/apache2/mods-available/mod-evasive.conf

-----------------------------------------------------------------------

<IfModule mod_evasive20.c>
    DOSHashTableSize    3097
    # blockage si un user charge 5 fois la meme page en 3 seconde
    DOSPageCount        5
    DOSPageInterval     3
    # blockage si un user charge 30 fois depuis le même site  en 1 une seconde
    DOSSiteCount        30
```

```
    DOSSiteInterval     1

    DOSBlockingPeriod   60

    DOSWhitelist        127.0.0.*

    DOSWhitelist        193.95.*

</IfModule>
```

❖ Paramétrage du mod-rewrite :

- On va adopter deux règles à appliquer pour chaque répertoire ou on veut l'appliquer. Lorsque l'on tape dans la barre d'adresse www.votre_domaine.net/index-* c'est la page www.votre_domaine.net/index.php?id=* qui s'affiche.
- Changer « .html » par « .php »

```
# vi /etc/apache2/sites-enabled/000-default

---------------------------------------------------------------------------

<IfModule mod_rewrite.c>

RewriteEngine on

RewriteRule ^(.*)\.html$ $1.php [nc]

RewriteRule ^index-([0-9]+)$ /index.php?id=$1 [L]

</IfModule>
```

❖ Paramétrage du mod-bandwith :

- On va donner une priorité aux visiteurs tunisiens

```
# vi /etc/apache2/sites-enabled/000-default

---------------------------------------------------------------------------

<IfModule mod_bw.c>
```

```
    BandwidthModule On

    ForceBandWidthModule On

    # ip tunisien sans limit

    Bandwidth 127.0.0.1 0

    Bandwidth 193.95.0.0/17 0

    Bandwidth 196.203.0.0/16 0

    Bandwidth 213.150.160.0/19 0

    Bandwidth 41.224.0.0/13 0

    Bandwidth 197.0.0.0/11 0

    # 1Mo pour le reste

    Bandwidth all 1024000

    # 1Mo pour les fichiers plus que 10 ko

    LargeFileLimit * 10240 1024000

    #garantir 5K par connexion

    MinBandWidth all 5120

</IfModule>
```

- Paramétrage du site :

```
# vi /etc/apache2/sites-enabled/000-default
```

```
<VirtualHost *:80>

    ServerAdmin webmaster@serveur.tn

    Options None

    #LimitRequestBody 10240
```

```
LimitRequestFields 40

LimitRequestFieldsize 512

LimitRequestline 20480

DocumentRoot /var/www/

<Directory />

Options FollowSymLinks

# Forbid default access to file system locations

Order Deny,Allow

Deny from all

# prevent use of .htaccess files in all directories

# apart from those specifically enabled.

AllowOverride None

</Directory>

<Directory /var/www/>

    <LimitExcept GET POST>

        deny from all

    </LimitExcept>

    Options +FollowSymLinks

    AllowOverride None

    Order allow,deny

    allow from all

    <IfModule mod_rewrite.c>
```

```
        RewriteEngine on
        RewriteRule ^(.*)\.html$ $1.php [nc]
        RewriteRule ^index-([0-9]+)$ /index.php?id=$1 [L]
    </IfModule>
    <IfModule mod_bw.c>
        BandwidthModule On
        ForceBandWidthModule On
        # ip tunisien sans limit
        Bandwidth 127.0.0.1 0
        Bandwidth 193.95.0.0/17 0
        Bandwidth 196.203.0.0/16 0
        Bandwidth 213.150.160.0/19 0
        Bandwidth 41.224.0.0/13 0
        Bandwidth 197.0.0.0/11 0
        # 1Mo pour le reste
        Bandwidth all 1024000
        # 1MO pour les fichiers plus que 10ko
        LargeFileLimit * 10240 1024000
        #garantir 5K par connexion
        MinBandWidth all 5120
    </IfModule>
</Directory>
```

```
        <Files *.inc>
            Order allow,deny
            Deny from all
        </Files>
#           ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
#           <Directory "/usr/lib/cgi-bin">
#                   AllowOverride None
#                   Options ExecCGI
#                       AddHandler cgi-script cgi pl py
#                   Order allow,deny
#                   Allow from all
#           </Directory>
            ErrorLog /var/log/apache2/error.log
            # Possible values include: debug, info, notice, warn, error, crit,
            # alert, emerg.
            LogLevel warn
            CustomLog /var/log/apache2/access.log combined
</VirtualHost>
```

- S'il ya un répertoire upload que le site utilise alors il faut empêcher l'exécution de scripts.

```
<Directory /var/www/upload/>
AddType text/plain .php .php .phtml .php3 .phps
</Directory>
```

4. OUTILS DE MONITORING

Il existe plusieurs méthodes pour surveiller apache :

- Un outil nommé « apachetop » indispensable pour surveiller apache.
- La deuxième façon est d'utiliser mod_status à partir des IP autorisées comme suit:

```
http://host/server-status?auto et http://host/ /server-status
```

- La troisième façon, c'est d'utiliser awstats, pour cela analyser le fichier/etc/awstats/awstats.conf et notamment SiteDomain= "www.serveur.tn" et DNSLookup=0

- La mise à jour des statistiques ce fait par :

```
#perl awstats.pl -config=mysite -update
```

- La quatrième façon on installe webalizer

```
#apt-get install webalizer geoip-bin libgd-tools

#rm –rf /var/www/webalizer

#mkdir /var/webalizer
```

- Puis changer les parameters dans /etc/webalizer/webalizer.conf

```
#LogFile /var/log/apache2/access.log

#OutputDir /var/webalizer

#HostName www.serveur.tn
```

- Les rapports seront générer quotidiennement dans /var/webalizer et il suffit de les uploader pour analyse, on déconseille de créer un alias pour accès web même avec restriction d'accès.

5. CONFIGURATION PHP

- Changement des quelques paramètres dans /etc/php5/apache2/php.ini

```
expose_php = Off

include_path = ".:/var/www"

safe_mode = On

safe_mode_include_dir = "/var/www"

safe_mode_exec_dir = "/var/www"

open_basedir = "/var/www"

safe_mode_allowed_env_vars = PHP_

disable_functions = exec,highlight_file,passthru,popen,proc_open,shell_exec,show_source,system

max_execution_time = 20

max_input_time = 30

memory_limit = 8M

post_max_size = 8M

upload_max_filesize = 2M

session.save_path = /var/lib/php5

output_buffering = Off

display_errors = Off

display_startup_errors = Off
```

6. CONFIGURATION DU FIREWALL, FAIL2BAN, CLAMAV, AIDE ET MISE A JOUR

1) Il faire un scan quotidien avec l'antivirus : clamscan /var/www/
2) Il faut vérifier quotidiennement le contrôleur d'intégrité disque : aide.wrapper|grep "www».
3) Fail2ban et déjà configurer pour ssh : /etc/fail2ban/jail.conf, /etc/fail2ban/filter.d/sshd.conf et /etc/fail2ban/filter.d/apache-auth.conf.

4) Il faut faire les mise à jours : apt-get update puis apt-get upgrade.
5) Pour la configuration du firewall Copier le fichier fw.sh /etc/init.d/

```
#chmod + /etc/init.d.fw.sh

#updataupdate-rc.d –f  fw.sh defaults

#fail2ban-client status
```

- Voici le fichier fw-web.sh

```
#!/bin/bash

export WEBMAXPERMIN="260" #nombre de paquets par ip source

export WEBBURST="40"

export WEBCONPERIP="16" nombre de connexions TCP simultanées par ip source

export IPT="/sbin/iptables"

export IPTS="/sbin/iptables-save"

export IPTR="/sbin/iptables-restore"

export LO_IF="lo"

export EXT_IF="eth0"

export LO_IP="127.0.0.1"

export EXT_IP=`ifconfig $EXT_IF | grep inet | cut -d : -f 2 | cut -d \  -f 1`

export CLASS_A="10.0.0.0/8"                  ## Réau de class A

export CLASS_B="172.16.0.0/12"               ## Réau de class B

export CLASS_C="192.168.0.0/16"              ## Réau de class C

export CLASS_D_MULTICAST="224.0.0.0/4"       ## Réau de class D

export CLASS_E_RESERVED_NET="240.0.0.0/5"    ## Réau de class E
```

```
export P_PORTS="0:1023"                    ## Ports privilege

export UP_PORTS="1024:65535"               ## Ports non privilege

export BLACK_LIST=""

export ADMIN_LIST="172.16.7.111"

export TUN_RANGE="193.95.0.0/17 196.203.0.0/16 213.150.160.0/19 41.224.0.0/13 197.0.0.0/11"

/sbin/modprobe ip_tables  || exit 1          ## Module principale iptables

/sbin/modprobe ipt_owner || exit 1           ## Correspondance avec le propriéire du paquet

/sbin/modprobe ip_conntrack  || exit 1       ## Suivie de connexion

/sbin/modprobe ip_conntrack_ftp  || exit 1   ## Suivie de connexion ftp

/sbin/modprobe ip_conntrack_irc || exit 1    ## Suivie de connexion irc

/sbin/modprobe ipt_LOG  || exit 1            ## Log des paquets

/sbin/modprobe ipt_REJECT  || exit 1         ## Refus de paquet avec erreur ICMP en retour

/sbin/modprobe ipt_MASQUERADE  || exit 1     ## Traduction d'adresse réau (NAT)

/sbin/modprobe ipt_TOS  || exit 1            ## Altétion du Type de Service (TOS)

/sbin/modprobe ipt_TCPMSS  || exit 1         ## Altétion du Maximum Segment Size (MSS) des TCP SYN

/sbin/modprobe ipt_MARK  || exit 1           ## Traçilitée certains paquets

/sbin/modprobe ipt_REDIRECT || exit 1        ## Redirection (ex: Proxy transparent)

/sbin/modprobe iptable_mangle  || exit 1     ## Atlétion des paquets (TOS & MMS)

/sbin/modprobe ip_nat_ftp  || exit 1         ## Traduction d'adresse réau pour le FTP

/sbin/modprobe ip_nat_irc || exit 1          ## Traduction d'adresse réau pour IRC

/sbin/modprobe ip_nat_snmp_basic || exit 1   ## Traduction d'adresse réau pou SNMP-NLG

/sbin/modprobe ip_queue  || exit 1           ## Passage des paquets en zone utilisateur (QUEUE)
```

```
/sbin/modprobe iptable_filter  || exit 1        ## Module principale iptables (Table filter)

/sbin/modprobe iptable_nat  || exit 1          ## Traduction d'adresse réau (NAT)

/sbin/modprobe ipt_ttl || exit 1               ## Correspondance en fonction du Time To Live (TTL)

/sbin/modprobe ipt_limit || exit 1             ## Limitation des correspondances (vs DoS)

/sbin/modprobe ipt_mac || exit 1               ## Correspondance avec l'adresse MAC du device

/sbin/modprobe ipt_multiport || exit 1         ## Gestion d'éelon de port

/sbin/modprobe ipt_length || exit 1            ## Correspondance

/sbin/modprobe ipt_hashlimit || exit 1            ## hashlimit

for T in filter nat mangle ; do

 $IPT -t $T -F

 $IPT -t $T -X

done

## Rèes par déut

$IPT -P INPUT DROP

$IPT -P OUTPUT DROP

$IPT -P FORWARD DROP

############################

## prise en charge des argument ##

############################

if [ "$1" = "stop" ]

then

            echo "Firewall désactivé."
```

```
# Suppression de toutes les chaînes pré-définies de la table FILTER
 $IPT -t filter -F
# Suppression de toutes les chaînes utilisateur de la table FILTER
 $IPT -t filter -X
# Par defaut, toute les paquets de la table FILTER sont acceptés
 $IPT -t filter -P INPUT ACCEPT
 $IPT -t filter -P OUTPUT ACCEPT
 $IPT -t filter -P FORWARD ACCEPT
# Suppression de toutes les chaînes pré-définies de la table NAT
 $IPT -t nat -F
# Suppression de toutes les chaînes utilisateur de la table NAT
 $IPT -t nat -X
# Par defaut, toute les paquets de la table NAT sont acceptés
 $IPT -t nat -P PREROUTING ACCEPT
 $IPT -t nat -P OUTPUT ACCEPT
 $IPT -t nat -P POSTROUTING ACCEPT
# Suppression de toutes les chaînes pré-définies de la table MANGLE
 $IPT -t mangle -F
# Suppression de toutes les chaînes utilisateur de la table MANGLE
iptables -t mangle -X
# Par defaut, toute les paquets de la table MANGLE sont acceptés
 $IPT -t mangle -P PREROUTING ACCEPT
```

```
        $IPT -t mangle -P INPUT ACCEPT
        $IPT -t mangle -P OUTPUT ACCEPT
        $IPT -t mangle -P FORWARD ACCEPT
        $IPT -t mangle -P POSTROUTING ACCEPT
        # Supprime du NAT dans le kernel
        # OK pour tout accepter, mais il ne faut pas rigoler quand même !
        echo 0 > /proc/sys/net/ipv4/ip_forward
        # Desactive les options anti-spoofing du kernel
        for Filter in /proc/sys/net/ipv4/conf/*/rp_filter; do
                echo 0 > $Filter
        done
        # Desactive les options anti-ping du kernel
        echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_all
        echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
        echo 0 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
        exit 0
fi
if [ "$1" = "bloc" ]
then
        # Suppression de toutes les chaînes pré-définies de la table FILTER
        $IPT -t filter -F
        # Suppression de toutes les chaînes utilisateur de la table FILTER
```

```
$IPT -t filter -X

# Par defaut, toute les paquets de la table FILTER sont détruits

$IPT -t filter -P INPUT DROP

$IPT -t filter -P OUTPUT DROP

$IPT -t filter -P FORWARD DROP

# Suppression de toutes les chaînes pré-définies de la table NAT

$IPT -t nat -F

# Suppression de toutes les chaînes utilisateur de la table NAT

$IPT -t nat -X

# Par defaut, toute les paquets de la table NAT sont détruits

$IPT -t nat -P PREROUTING DROP

$IPT -t nat -P OUTPUT DROP

$IPT -t nat -P POSTROUTING DROP

# Suppression de toutes les chaînes pré-définies de la table MANGLE

$IPT -t mangle -F

# Suppression de toutes les chaînes utilisateur de la table MANGLE

$IPT -t mangle -X

# Par defaut, toute les paquets de la table MANGLE sont détruits

$IPT -t mangle -P PREROUTING DROP

$IPT -t mangle -P INPUT DROP

$IPT -t mangle -P OUTPUT DROP

$IPT -t mangle -P FORWARD DROP
```

```
        $IPT -t mangle -P POSTROUTING DROP

        # Supprime du NAT dans le kernel

        echo 0 > /proc/sys/net/ipv4/ip_forward

        # Active les options anti-spoofing du kernel

        for Filter in /proc/sys/net/ipv4/conf/*/rp_filter; do

                echo 1 > $Filter

        done

        # Active les options anti-ping du kernel

        echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all

        echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

        echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

        exit 0

fi

if [ "$1" = "start" ]

then

echo "1" > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

echo "0" > /proc/sys/net/ipv4/conf/all/accept_redirects

echo "1" > /proc/sys/net/ipv4/conf/all/log_martians

echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

echo "1" > /proc/sys/net/ipv4/conf/all/rp_filter

echo "0" > /proc/sys/net/ipv4/conf/all/accept_source_route

echo "0" > /proc/sys/net/ipv4/tcp_ecn
```

```
#echo "16384" > /proc/sys/net/ipv4/netfilter/ip_conntrack_max

echo "1" >/proc/sys/net/ipv4/tcp_syncookies

echo "1" >/proc/sys/net/ipv4/conf/all/secure_redirects

echo "0" > /proc/sys/net/ipv4/icmp_echo_ignore_all

#       echo -e "32768\t61000" > /proc/sys/net/ipv4/ip_local_port_range

$IPT -N BLACKLIST

$IPT -F BLACKLIST

$IPT -N out_apache

$IPT -F out_apache

#$IPT -N  fail2ban-ssh

#$IPT -F fail2ban-ssh

#$IPT -A INPUT -p tcp -m multiport --dports 22 -j fail2ban-ssh

#$IPT -A fail2ban-ssh -j RETURN

$IPT -N throttle

$IPT -F  throttle

$IPT -A throttle -m hashlimit \

 --hashlimit-name webthrottle \

 --hashlimit-upto $WEBMAXPERMIN/minute \

 --hashlimit-mode srcip \

 --hashlimit-burst $WEBBURST \

 --hashlimit-htable-expire 300000 \

 -j ACCEPT
```

```
$IPT -A throttle -j LOG --log-prefix "FREIN " --log-level 1

$IPT -A throttle -j REJECT

$IPT -A BLACKLIST -d $CLASS_D_MULTICAST -j DROP

$IPT -A BLACKLIST -d $CLASS_E_RESERVED_NET -j DROP

for NET in $BLACK_LIST; do

   $IPT -A BLACKLIST -d $NET -j DROP

   $IPT -A BLACKLIST -s $NET -j DROP

done

$IPT -A OUTPUT -j BLACKLIST

$IPT -A OUTPUT   -m state --state ESTABLISHED,RELATED -j ACCEPT

$IPT -A  OUTPUT -m owner --uid-owner www-data -j out_apache

$IPT -A  OUTPUT -m owner --uid-owner root -j ACCEPT

$IPT -A out_apache -p tcp --syn -d 127.0.0.1 --dport 3306 -j ACCEPT

$IPT -A out_apache -p tcp --syn -d 127.0.0.1 --dport 25  -j ACCEPT

$IPT -A out_apache -j REJECT

$IPT -A INPUT -j BLACKLIST

$IPT -A INPUT -s $LO_IP -j DROP

$IPT -A INPUT -s $CLASS_A -j DROP

#$IPT -A INPUT -s $CLASS_B -j DROP

$IPT -A INPUT -s $CLASS_C -j DROP

$IPT -A INPUT -s $CLASS_D_MULTICAST -j DROP

$IPT -A INPUT -s $CLASS_E_RESERVED_NET -j DROP
```

```
$IPT -A INPUT -m limit --limit 3/m -m state --state NEW -p TCP --tcp-flags ! ALL SYN -j LOG --log-prefix="INVALIDE_SYNC "

$IPT -A INPUT -m state --state NEW -p TCP --tcp-flags ! ALL SYN -j DROP

$IPT -A INPUT -m limit --limit 1/m -m state --state INVALID -j LOG --log-prefix="INVALID_CONNECTION "

$IPT -A INPUT -m state --state INVALID -j DROP

$IPT -A INPUT -p icmp --icmp-type echo-reply -m limit --limit 3/minute --limit-burst 5 -j ACCEPT

for NET in $ADMIN_LIST; do

   $IPT -A INPUT  -s $NET -j ACCEPT

done

for NET in $TUN_RANGE; do

        $IPT -A INPUT -m state --state RELATED,ESTABLISHED,NEW -p tcp -m tcp --dport 80 -s $NET -j ACCEPT

done

# nombre max de connexion par IP sources

$IPT -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above $WEBCONPERIP -j REJECT

$IPT -A INPUT -m state --state RELATED,ESTABLISHED,NEW -p tcp -m tcp --dport 80  -j throttle

$IPT -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

        exit 0

fi
```