Sécurité kernel

Options kernels à utiliser pour restreindre des comportements de routage, ICMP… inutiles à proposer.

Backuper le fichier original mais ne pas le modifier.

```
cp -p sysctl.conf sysctl.conf.orig
```

Pour de nombreux paramètres réseaux, configurer le fichier suivant qui liste les paramètres kernel à exécuter au démarrage.

```
vi /etc/sysctl.d/custom.conf
```

```
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.ip_forward = 1 #Inclus la ligne suivante :
net.ipv4.conf.docker0.forwarding = 1
net.ipv6.conf.all.forwarding=0
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.all.proxy_arp = 0

##################################################################
# Custom
vm.swappiness=2
```

Pour charger la configuration modifiée sans redémarrer.

```
sysctl -p
```

`sysctl.conf` complet.

```
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
```

```
############################################################3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path
filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=0

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
net.ipv6.conf.all.forwarding=0

###################################################################
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
# _or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
net.ipv4.conf.all.secure_redirects = 0

# gateway list (enabled by default)
net.ipv4.conf.all.secure_redirects = 0
#
# Do not send ICMP redirects (we are not a router)
net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (we are not a router)
net.ipv4.conf.all.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
#
# Log Martian Packets
net.ipv4.conf.all.log_martians = 1
```

```
#
# Proxy ARP
net.ipv4.conf.all.proxy_arp = 0

###################################################################
# Magic system request Key
# 0=disable, 1=enable all
# Debian kernels have this set to 0 (disable the key)
# See https://www.kernel.org/doc/Documentation/sysrq.txt
# for what other values do
#kernel.sysrq=1

###################################################################
# Protected links
#
# Protects against creating or following links under certain conditions
# Debian kernels have both set to 1 (restricted)
# See https://www.kernel.org/doc/Documentation/sysctl/fs.txt
#fs.protected_hardlinks=0
#fs.protected_symlinks=0

# Disable IPv6 autoconf
net.ipv6.conf.all.autoconf = 0
net.ipv6.conf.default.autoconf = 0
net.ipv6.conf.eth0.autoconf = 0
net.ipv6.conf.all.accept_ra_defrtr = 0
net.ipv6.conf.default.accept_ra_defrtr = 0
net.ipv6.conf.eth0.accept_ra_defrtr = 0
net.ipv6.conf.all.accept_ra_pinfo = 0
net.ipv6.conf.default.accept_ra_pinfo = 0
net.ipv6.conf.eth0.accept_ra_pinfo = 0
net.ipv6.conf.all.accept_ra = 0
net.ipv6.conf.default.accept_ra = 0
net.ipv6.conf.eth0.accept_ra = 0
```

Différence de conf entre une installation originale Debian 9 et les modifications appliquées (Original à gauche, modifié à droite).

```
net.ipv4.conf.all.forwarding = 1                  |
net.ipv4.conf.all.forwarding = 0
net.ipv4.conf.all.log_martians = 0                |
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.all.rp_filter = 0                   |
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.secure_redirects = 1                |
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 1                  |
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.forwarding = 1                  |
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.default.rp_filter = 0               |
```

```
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.docker0.forwarding = 1                  |
net.ipv4.conf.docker0.forwarding = 0
net.ipv4.conf.eth0.forwarding = 1                   |
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.lo.forwarding = 1                     |
net.ipv4.conf.lo.forwarding = 0
net.ipv4.ip_forward = 1                           |    net.ipv4.ip_forward = 0
net.ipv6.conf.all.accept_redirects = 1                  |
net.ipv6.conf.all.accept_redirects = 0
```