

#####

```
##### <ale@FreeBSD.org>
#####: 43126
```

#####.

3### ### ##### ### ##### ##### ## 3### ###-
#####.

```
#####, #####, #####, #386, #486, #####, #####, ##  
#### ## ##### ## ##### ##### ## ##### ##-  
##### ## ## ##### ## ## ##### ##### ## ##  
#####.
```

```
#####  
#####  
#####  
#####
```

2013#11#07 ### #####.

#####

```
##### ## ## ##### ## ##### ## ##### ##### (#####
## #####) ## ##### ##### ##### ##### ##
##### ## #####, ## ##### ## ##### ##### ##-
#####. ## ##### ## ##### ## ##### ##
##### ##### ## #####. ## ##### ##### ##
##### ## ##### ## ##### ## #####.
```


 (#####) ## ##### ##### # ##### ## ## #—
 ##### ## ##### ##### ##### #####
 ##### ## ## ##### ## ##### #####
 ##### #####. ##### ##### ## #####
 ##### ## ##### (#####) #####
 #####.

Version française de Marc Fonvieille <blackend@FreeBSD.org>.

#####

1. ##### ## #####? 2

2. #####	2
3. #####	3
4. ##### ##	5
5. ##### ##	5
6. #####	8

1. ##### ##### ## #### #####?


#####, ##### # ## ##### ### ##### ## #####—
(####) ## ##### ## ##### ## ## ##### ### ##### ####4 #####—
#####, ##### ## ##### ### ##### # ##### 24 ##### ## 24 ##
(##### #### ## ## ##### ## 2) ##### ##. #### ## #####

#####, ##### ## ##### ## ##### ## ##### ##—
#####, ##### ## ##### ## ##### ##
#####, ## ##### ##### ## ##### ##### (##), ## ##### ##
#####. ##### ## ##### ##### #####
#####.

#####/##### ##### ## #####
####.

2. #####

#####. ##—
4.5##### ## ## ##### ## #####
#####, #####
#####. ##### ## ##### #####
#####.



#####

Ne pas #####: ## ##### exclue #####.
#####—
####.

#####, ##### ## ## ##### ##### ##### ## ##—
#####, #####
#####

#####

#####, ## ### ### ##### ##### ## ####, ## ####, ##### ## ##### #####
(### ## #####). ###
#####TM ###, ##### ## ## #####
3#9## ## ##### 3###@. ##### ##### ## ##### ## #####
(##### ## ##### ## #####
#####) ##### ## ##### ##### ##### ##### ## #####
#####.

2.1.

#####. ####
#####, ##### ##### ## ##### ## ##### ## #####
#####:

```
options BRIDGE
options IPFWALL
options IPFWALL_VERBOSE
```

####, ## ##### ## ##
#####.

#####. ####
##—
#####.

2.2. ##

#####; ## #####
/boot/loader.conf:

```
bridge_load="YES"
```

#####, ##### ## ##### ## ##### ## ##### bridge.ko #####
#####. ## ##### ## ##### ## ##### ## ##### ipfw.ko,

#####.

3.

(##### ## ##### #####), #####
/etc/rc.conf. ## #####
##. ## ##### #####
#####, ##### ## ##### #####
(##### ## ## ## ##### ##,

#####

```
#####)#####  
##### /etc/rc.conf:
```

```
firewall_enable="YES"
firewall_type="open"
firewall_quiet="YES"
firewall_logging="YES"
```

```
## ##### ##### ## ##### (# ##### ## ##### ipfw.ko #####
##### ## ##### ## #####), ## ##### ## ##### ##### ## #####
##### (##### ##### #/etc/rc.firewall), ## ##### ##### ## #####
## ##### ##### (#####) ## ## ##### ##### ## ##### ##
##### ##### ## #####.
```

[illegible]

#####. ##### ## ##### ##### ## #####—
###, ## # # ## ##### ##### ##### ##### #####: ##### ## ##, #####
#####. ## ##### ## ##### ## ##### ## ##### ## ## #####
(#####). ##### ##### ##### ##### ##### #####—
##, ## ## ##### ## ## ##### ##### ## ##### ##. ## ##
##, ##### ##### #####
#####. ## ##### ## ##### #####—
(### #####) #####
#####, ##### ## ##### ## ##### ## ## #####—
###.

```
## ### ##### ## ##### ## ##### ## ## ##### ##### ##-
#####: ## # #### ## ##### ##### ##### ## #### ## ## #####, ####
## #### ## #### ## ##### ## ## #####, ##### ## #### #####, #####
##### #####.
```

#####

#####, #### ##### ## ##### ##### ##
#####.

4. ##### ##

####, #### ##### ## ####, #### ##### ## ##### #####
(## ##### ## ##### ## ##### ## ##### ## ##### fxp0 ## xl0 ##
#####):

```
# sysctl net.link.ether.bridge.config=fxp0:0,xl0:0
# sysctl net.link.ether.bridge.ipfw=1
# sysctl net.link.ether.bridge.enable=1
```

##,

#####.



####

5.1##### ## ## #####-
#####, ## #####. ##### ## ##
[#####\(4\)](#) #####.

##, #### ##### ## ##### ## ##### ##-
##-
#####, ##### ## ##### ## ##### net.link.ether.bridge.[bla]=[bla] ## ##
/etc/sysctl.conf ## ## #####.

5. ##### ##

#####, #### ## ##### ## #####. ## # ## #####-

##. ## ##, ## # ## ##### ## ##

#####, ## ##### ##### ## ##### ## ## ##,
##; ## ## ## ## ## ##, ##-
#####. #####,

#####. ## ##### ## ## ## ## ## ## ## ##
##.

#####

```
##### ## ##### # #####. ##### ##### ##### ##### # #####
/etc/rc.firewall ## # # #### # ## ##### ##### ##### # #####
lo0, ##### # # ##### # # #####. ### ##### ##### #—
##### # ## ##### # # ##### (##### /etc/rc.firewall.local) # #####
# ##### #, # ##### # ##### # /etc/rc.conf # #####
# #####.
```



```
#### ##### ##### ## ##### complet, ##### ## ## ##### ##
##### ##### ## ##### ## ##### ##### ## #####.
```

```
# Les choses dont nous avons gardé l'état avant de
continuer
add check-state
```

6

#####

```
add drop all from 192.168.0.0/16 to any in via fxp0

# Autorise la machine pont à communiquer si elle le désire
# (si la machine est sans adresse IP, ne pas inclure ces lignes)
add pass tcp from 1.2.3.4 to any setup keep-state
add pass udp from 1.2.3.4 to any keep-state
add pass ip from 1.2.3.4 to any

# Autorise les hôtes internes à communiquer
add pass tcp from any to any in via xl0 setup keep-state
add pass udp from any to any in via xl0 keep-state
add pass ip from any to any in via xl0

# Section TCP
# Autoriser SSH
add pass tcp from any to any 22 in via fxp0 setup keep-state
# Autoriser SMTP seulement vers le serveur de courrier
add pass tcp from any to relay 25 in via fxp0 setup keep-state
# Autoriser le transfert de zone seulement par le serveur de noms esclave [dns2.nic.it]
add pass tcp from 193.205.245.8 to ns 53 in via fxp0 setup keep-state
# Laisser passer les sondes d'ident. C'est préférable plutôt que d'attendre
# qu'elles s'arrêtent
add pass tcp from any to any 113 in via fxp0 setup keep-state
# Laisser passer la zone de -"quarantaine"
add pass tcp from any to any 49152-65535 in via fxp0 setup keep-state

# Section UDP
# Autorise le DNS seulement vers le serveur de noms
add pass udp from any to ns 53 in via fxp0 keep-state
# Laisser passer la zone de -"quarantaine"
add pass udp from any to any 49152-65535 in via fxp0 keep-state

# Section ICMP
# Laisser passer -'ping'
add pass icmp from any to any icmptypes 8 keep-state
# Laisser passer les messages d'erreurs générés par -'traceroute'
add pass icmp from any to any icmptypes 3
add pass icmp from any to any icmptypes 11

# Tout le reste est suspect
add drop log all from any to any
```


#####

```
add deny all from 1.2.3.4/8 to any in via fxp0
```


#####

au moins ## #### ## ##### #### #### # ####
#####: ## #####. #### #####, ## #####
####, ##### ## #####
####.

####, ##
#####. #### # # ##
#####: #### ## #####.

####, ## #####. #####
#####, ##### ##
(## ##### ## ##### ##### ## ##
###(8)). ##### ## ##### ## #####
avant ## ## ##

#####. ##### ## ## #####
(##### ## ## #####).

##—
(## #### 113). #####,

#####. ##### ## ##

113, ## ## ##
(## #####).

#####. ##### ## ## ##
##—

#####.

6.

#####.

