#######

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

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

3### # ########## #### ###### ########## ##### 3### #####–
######.

#####, #######, ############, #386, #486, #######, #######, #
###########
#####.

###–
######.
#####, # ## ####### #######
#######, ####### ##### ####### ### #######
###.

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

########

(#### ### ########)
########, ##### ##### ###### ######### #
#######. ## ########### ###
######. ##
####### ### ### ########## ## #### # ########### ### #######–
#####.

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

######

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

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

###/###### ######## ##### ##### ######## ## ########–##### ## ######### ##.

####

#####–####, *non* ##### ## ###### #### ##### #######. ### ##### ##############, ########, ######## # ######## ######## ##### #### ###### ######### ## #### ## ### ###### ########## # ##–#######.

2. ######

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

##########

Non ####### ######## ## ##########: ## ######### #### a esclusione. ######### ############# ### ###### ## ###### #### ###### ######## # ########.

#######–#####, ####### ###### ###### ## ##### ## ####### ######### ######## ### ######–### #########, ### #### ## ####. #######, ### ##### ## #### ##########, ## ###### ########## ###### ## #### ### ### #########. ## ###### ######## #### ###### ## ##### ############™ ### ####### ##### 3###® 3#9## ###### ####. ### ######## ##### ############## ### ######## ### ###### ##### ##### ### ###### ## ###### ########## (### ##### ####### ##########) ## #### ## ########## ########## ##### ########## ### ######### ## ###### # ##### #### #### #######.

2.1. ############## ###

######–#######. ### ##### #### ####### ########## ## ######## ##### ## #### ## #####–######### ### ######:

```
options BRIDGE
options IPFIREWALL
options IPFIREWALL_VERBOSE
```

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

######. ## ####### ###–#### ## ########## ##### ####### ######## ### ########## # ###### ###### #############.

2.2. ########### ###

#############, ######## #### ## #### # ########## ## ######## #### ## #### /boot/loader.conf:

```
bridge_load="YES"
```

bridge.ko. ### # ########## ###### ########## ### #### ### ## ###### ipfw.ko ## ###### ##### ######## ## ########## ##### ###### /etc/rc.network #### #### ######## # ##### ##### ######## #######.

3. ##########

(# ######## ### ###### ### ##### ###### ## ##########), ####### ########## ###### ######### ## #### /etc/rc.conf. ## ###### ## ######## ### ######## # ## ######### ##### # ###–###### ##. ### ######## ######### ## ######## ## ######## open, ## #### ## ####–###### ## ### ############## ##### ##### ######## ## ########## ######### (### #### ###### ######### ###### ######### ## ######, #### ############ ## ######–#### ## ### ######## ############ ######## ##### ##### ####). ######## ###### ##### ### #### /etc/rc.conf:

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

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

####, ## ###### ### ########## # ###### ## ######### ## ## # #### ### ##### ###### ## ####, ## ## ####–## ######## ########## ##### ## ######## # ######## ##### ########## ## ## ###–####. ## ############ #### (#######) ## ######## ###### #### ###### ### ######## ## ###### ############## ##### ####: ### ############ ######### ###### ######## ## ######## # ######## ### ##### ########### ## #### ######## ### ######. # ##### ######### ##### ######## ######## ######### ######## ## ######## #### ####, ### ######## ### ### ############ ## #######: ## ###### #### # ########## ######### ## ## ############### ######## (###### ######### # ########, #### ######## ## ###–### ###), ##### ### ## ###### ##### ######## #### #### ##### ######### ## #####. ###### #### #### ### ############## fxp0 (### ###### ####) #### ###### ########## ##### ######## ######## ### #### /etc/rc.conf, ###### ## xl0 ##. ######### ## # ######## ## ###### ## #### ### ## ##### #####, # #### ### ######## ## ######### ## ##### ### ## ##### ######## # ######## ######## ## ######## # ######## ########.

######. ###### ## ######## ## ##### ######## ## #### ### ########## ######## ## ###: ### # ##, ######## # ###. ### ######## ## ###–######## ############### ## ## ### ######## ### ### ######### ######## (######## ###). ######## ### ######## ######## ### ###### ######## # ########## ### #### # ########## ### ## ###### ##### ######## # ######### ###. #### ########## ### ## ##### ### ######## ##, ##### ### # ######## #### ### ## ##### ########. ## ######## ## ######## ###### ############### ### ######## ## # ###### ##### # ######### ### ## (######### ###) ######## ######### ##### ###### ########, ##### ## ## ######## # ############ ### ### ######## ######## #####.

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

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

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.[blah]=[blah] ## ###### ##### ## #### /etc/sysctl.conf, ## #### ### ######## ######## ######### ##### ########.

5. ############## ###

########, ## #### ## ######## ###### ## #### ########. ## #### ##### ############## ### ##– ## ######, ###### ### ##### ## ############ ### ######## #### ########### ### ######### ######### ### ######. ########, ### ### ########## ### # ######### ### ###### ### ###### ######### ### ###### # ###### ########### #### ######## ##– ####. ## ########, # ######### ### ######## ### ###### ######## ########## ### ##–

#####, ### ### #### ## ######; ####### ####### ######## #### ## ########, ###### ######### ###### ### ### out ###### xmit ### ##### ### ########. ############# ### in via ### # ### ######## ### ######, ## ### ## ## ##### ###### ## ## #####. ######## ########## # ### ## ####### ##### #### # ####### pass # drop ### # ######### ######## ### ######. #### ######## #### divert, forward # reject ### #### ##########. ###### ####### ####### ###### ###### #####, ## #### ### ## ######## ## # ##### ## ######## ###### ###### (###### ### ## ### ##### ######### ## ##).

4.0 # ## ######## ## ######## #########. ###### # ## ###### ##–########## ### ## ######## ###, ### ######## ########## ## ### ######### ## ######, ####### # ##### ####### ## ### ######## ### ## ###### ###### ## #######–## ## # ###### ## ##### (## ### ######## # ########### #########, ##########). ### # ######## ### ### ########## ## ########### ## #####, ### ### #### ## ##–##### ###### ##### ####### ## #### #### ### ######## #####. ## ### ## ######## ### ### ############ ## ## ######### ### ## ###### # ######## ### ######## ### ###### ##########, ####### # ####### ### # ########. ######### ######## ###### #### ####. ## ###### #### # ######### ##### ### # ######### ###. ###### ######## ## ####### ####### #### ## ####### ###### ## ####### # ##### ####### #######, ## ########### ## ##### ######## ########### ## ####### ## #####.

####### ## ####### ## ###############. ####### ###### ### ########## ### #### / etc/rc.firewall ## #### ### ##### ###### ######## ### ############# ## ######## lo0, ###### ### ## ## ########## ### ###. ## ###### ############## ########## ##### ## ## #### # ##### (### ####### /etc/rc.firewall.local) # ######## ######### ########### ## #### ### #### /etc/rc.conf #### ### ##### ######## ## ######## open ###:

```
firewall_type="/etc/rc.firewall.local"
```

##########

####### ########### ## #### *completo* ### ####, ########## ### ##### ######## ### ## ####### ## ######## ######## ##### ##### ####.

fxp0 ######### ########### (########) # ## xl0 ##### ######### (###). ## ######## ###### ## ####–##### #### 1.2.3.4 (# ########### ### ## ###### ### ## ####### ## ######### ###### # ######, ## ### ######### ## ####).

```
# Le connessioni di cui abbiamo mantenuto lo stato vengono fatte passare subito
add check-state

# Esclude le reti locali definite nell'RFC 1918
add drop all from 10.0.0.0/8 to any in via fxp0
```

```
add drop all from 172.16.0.0/12 to any in via fxp0
add drop all from 192.168.0.0/16 to any in via fxp0

# Permette alla macchina bridge di connettersi con chi vuole
# (se la macchina è IP-less non includere questi comandi)
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

# Permette agli host della rete interna di connettersi con chi vogliono
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

# Sezione TCP
# Permette SSH
add pass tcp from any to any 22 in via fxp0 setup keep-state
# Permette SMTP solo verso il mail server
add pass tcp from any to relay 25 in via fxp0 setup keep-state
# Permette i trasferimenti di zona solo dal name server secondario [dns2.nic.it]
add pass tcp from 193.205.245.8 to ns 53 in via fxp0 setup keep-state
# Lascia passare i controlli ident:
# è meglio che aspettare che vadano in timeout
add pass tcp from any to any 113 in via fxp0 setup keep-state
# Permette connessioni nel range di -"quarantena".
add pass tcp from any to any 49152-65535 in via fxp0 setup keep-state

# Sezione UDP
# Permette DNS solo verso il name server
add pass udp from any to ns 53 in via fxp0 keep-state
# Permette connessioni nel range di -"quarantena".
add pass udp from any to any 49152-65535 in via fxp0 keep-state

# Sezione ICMP
# Abilita le funzioni di -'ping'
add pass icmp from any to any icmptypes 8 keep-state
# Permette il passaggio dei messaggi di errori del comando -'traceroute'
add pass icmp from any to any icmptypes 3
add pass icmp from any to any icmptypes 11

# Tutto il resto è sospetto
add drop log all from any to any
```

########. ## ##########, ### ## #### ###### ###### ## ########, ##–##### *non* ####### ########:

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

######, ### ### ####### ########### ######### ### ######### ## ###### ###–## #### #######. ###### # ### #### ### ########## ##### ##### ### ###### ##–#### ### ######## ### ##### # ####### ## ###### ######, ######### ##### ###–

############. ## ######## # ### ### *almeno* ## #### ################ ####### ### ### ## ### ########: ## ######. ############, ####, ### ### ######## ## ######### ########## ### #### ###### # ###### ### ## ## ###–##### ###########.

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

######, ## ## #####. ########## ######## ### ## ###### #### ###### #######–####### ### ## ####### ########, ###### ### # ##### ### ### ######### ####### (## ####### ##### ###### # ######## ################ ##### ### #### ####(8)). ####–### ###### ###, ######## ######## # #### ##### ############ ############, ## ##–######### ### #### #### ########## *prima* ### ## ###### ### ########. ###### # ## ###### ####### ### ######## ############ ## ####### #### ##### ######## ####–## ## ####. ## ########### # ######### ########## ############ ########## ## ####### ## #### #### (#### ########## ## ## ######## # #######).

###–### ##### ### ###### reset # forward ### # ######### ##### (##### 113 ###). ######–#########, ###### ### # ### ###### ########## ### ## ######, ###### ## #### ##–###### # ######### ######## #### #### ############. ###### ## ######## ## #####–####### ### ## ## ###### ##### ######, ###### ####### # ############ ######. ############# # ######## ## ########## ##### ##### 113, ####### ####### ###–##### ### ####### #### ### (## ######### ##### ###### ###### ## #######).

####### ##### #### ## ### ########## ### ###### #### ###### # ### ### ### ##–#### ### ####### ########## ## ######## ###### # ######## ### ### #### ##### #### ######. ######### ### ###### # ###### ## ##### ### # ### #### ## ######## ######## ######## ########## ########## ## ###### # ## ########## ##### ###–### ## ###### ######. ## #### ####### ####### ########## ## ######, ###### ## ######## ###### ##### ## ####### ##### ## ### ## ##########. ###### ### ###### ### ####### ### #### ##########. ## ###### in via fxp0 ########## ## ######## # ##–##. ## ########, ## ##### ###### in via ########## ## ###### ######, ####### #### ############ ### # ######### ######## ##########, ## ###### ### ####### #####–## ####### ###########.

6.

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

######–
##
########.