#########
(######### #######)

<ale@FreeBSD.org>
#######: 52261

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

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

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

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

2018#09#16 01:21:25 ### #######.

######

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

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

######

1. ### ### #### ### ##### ## #########? 1
2. #### ######## 2
3. ########## ##### 2
4. ########### # ##### 3
5. ############ # ######## 4
6. ############## 6

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

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

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

2. ####

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

##########

Não #### ## #### ##########: ## ############ *exclui* # #####. ######### # ###### ##### ## ###### ### #### ############ # ###########.

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

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

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

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

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

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

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

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

```
bridge_load="YES"
```

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

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, forwar ## 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 (### # ######## ### # ### ### ##### ### ### ## ######## #####, ### #### ##### ######## ### # ###).

```
# Things that we have kept state on before get to go through in a hurry
add check-state

# Throw away RFC 1918 networks
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

# Allow the bridge machine to say anything it wants
# (if the machine is IP-less do not include these rows)
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

# Allow the inside hosts to say anything they want
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

# TCP section
# Allow SSH
add pass tcp from any to any 22 in via fxp0 setup keep-state
# Allow SMTP only towards the mail server
add pass tcp from any to relay 25 in via fxp0 setup keep-state
# Allow zone transfers only by the slave name server [dns2.nic.it]
add pass tcp from 193.205.245.8 to ns 53 in via fxp0 setup keep-state
# Pass ident probes.  It is better than waiting for them to timeout
add pass tcp from any to any 113 in via fxp0 setup keep-state
# Pass the "quarantine" range
add pass tcp from any to any 49152-65535 in via fxp0 setup keep-state

# UDP section
# Allow DNS only towards the name server
add pass udp from any to ns 53 in via fxp0 keep-state
# Pass the "quarantine" range
add pass udp from any to any 49152-65535 in via fxp0 keep-state

# ICMP section
# Pass 'ping'
add pass icmp from any to any icmptypes 8 keep-state
# Pass error messages generated by 'traceroute'
add pass icmp from any to any icmptypes 3
add pass icmp from any to any icmptypes 11

# Everything else is suspect
add drop log all from any to any
```

####### ## ##### ### ## ############ ######### ##### ##### ##### ####### ###### ### ##### ########. ## ##########, ### ## ###### #############, ## ####### ### *não* ###########:

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

####, ###### ## ####### ### ##### ##### ## #### ## #### ####### ### ## ##### ####. #### # #### ### #### ########## ##### #### ### ####### ## ### ###### ### ######## ####### ## ###### ## #######, ####### ####### ######## ### ####### ### ## ######. # ######## # ### ###### *pelo menos* ## #### ## ######### ####### ### #### ### ###### #######: # ########. ### ########## ### ### ########## ## ### ########, ##### ### ########## ### ######### #####.

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

####### #### ###### #### ###### # ####### #### # # ## ### #### # ######## ## ###### # # ######## ## #####, ## #### ## #####. ##########, #### # ######## ## ###### #### ### ######## ## ###### ### ## #### ########### ########, #### # ###### ## ####### ########## (# ####### ## ##### # ######## ### ######## ## ###### ## ###### ## ####(8)). #### ###, #### ### # ####### # # #### #########, ## ######### ## ######## ## ##### ##### ######### *antes* ## ##### ### ########. #### # ## ####### ## ###### #### ####### ### ######## ## ### ####### # ## ## ##### ## #### #######. #### ###########, # ######## ########## # ######## ## ## ### ## #### ## #### (########## ## # ####### ### ##### ##).

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

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

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

6.

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

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

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