#######

<ale@FreeBSD.org>
########: 53993

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

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

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

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

2020#03#19 09:04:27 ### ##########.

########

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

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

##########

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

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

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

######. ## ############ ##### ## ###### #### # ## ###/###### ########, ######## ### ######### ## ########## ##.

2. ####### ##

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

##########

No #### ##### #############: ## ############# *excluye* ## ####. ########## ## ##### ###### ## ####### # ### ########### # ###########.

###########, ## ### ##### ##### ###### ######## ######## ### ######### #########, ## #### ## ####. ######, #### ##### ### ##### #### ## #############, ### ######## ##### ### ######## ### ### ###. ### ######## ######## ###### ###### ##### ############™ ###, ######## ## ## 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
```

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

#####– ## ######### ## ############ ##### #####. ## ## ##########, ## ######### #### ## ###### ## ######### net.link.ether.bridge.*[blah]=[blah]* ## ######## /etc/sysctl.conf, #### ### ## ####### ## ######.

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

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

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

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

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

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

##########

completa, ## ## #########, ## ## #######, ### ## ###### ## ########## ####### ## ## ###.

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

```
# Cosas para las que tenemos que mantener el estado
add check-state

# Desechar todas las redes 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

# Permitir que la máquina bridge diga lo que quiera
# (si la máquina es IP-less no incluya estas líneas)
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

# Permitir que los hosts internos digan lo que quieran
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

# Sección TCP
# Permitir SSH
add pass tcp from any to any 22 in via fxp0 setup keep-state
```

```
# Permitir SMTP solo hacia el servidor de correo
add pass tcp from any to relay 25 in via fxp0 setup keep-state
# Permitir transferencias de zona solo por el servidor de nombres esclavo [dns2.nic.it]
add pass tcp from 193.205.245.8 to ns 53 in via fxp0 setup keep-state
# Dejar pasar ident probes. Es mejor que esperar a que se agote el tiempo
add pass tcp from any to any 113 in via fxp0 setup keep-state
# Dejar paso al rango "quarantine"
add pass tcp from any to any 49152-65535 in via fxp0 setup keep-state

# Sección UDP
# Permitir DNS solo hacia el servidor de nombres
add pass udp from any to ns 53 in via fxp0 keep-state
# Dejar pasar el rango "quarantine"
add pass udp from any to any 49152-65535 in via fxp0 keep-state

# Sección ICMP
# Dejar paso a 'ping'
add pass icmp from any to any icmptypes 8 keep-state
# Dejar paso a los mensajes de error generados por 'traceroute'
add pass icmp from any to any icmptypes 3
add pass icmp from any to any icmptypes 11

# Todo lo demás es sospechoso.
add drop log all from any to any
```

######## ## ######## ### ###### ######### ######### ###### ######## ### ###### ######## ######. ## #####–#####, ## ### ###### ###### ## ############ ## #########, ## #####, *no* ### ########:

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

#####, ######### ### ######## ### ###### ### ######## ######## ########## # ######## ###. #### ## #### ### ############ ###### #### ########## ## ### ######## ## ###### ## ###### ## ######## ## ########, ######### ######## ######### ### ######## ### ## ###### ## ## ###. ## ######## ## ### ### *al menos* ## #### ## ## ######## ######## ### ## ###### ########: ## ######. ####, ### ## ########, ## ### ###### ###### ###### ## ############ ## ######### ## ## ######, ### ## ### ## ######## ### ############ ############.

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

########, ## ###–#### ## #####. ########## #### ## ######## ## ###### #### ### ######## ## ######## ### ### ############ ##########; #### ## #### ## ######## ########## (## ######## ## ## ###### ## ######### ### ######### ## ## ###### ### ###### ## ####(8)). ###### ## ###### ### #### ### ## ######## # ## #### ######### ### ######–### ### ######## ## ######## ###### ######### *antes de* ### ## ###### #### ########. #### ## ## ######## ## #### ########## ## ########## ## ## ## ## ######## ## ### ########. #### ###### ## ###### ### ###### ###### ########### ## ######### ## ## ###### ### ###### ### #### (######### ## ## ######## ## ###### ##).

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

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

6.

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

#########.

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