##########

<sysadmin@alexdupre.com>
######: 43126
2013#11#07 ######### #####.

########

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

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

######

1. ######## ######## ### # ###### ############? 1
2. ########## 2
3. ############# ## ##### 3
4. ############ ##### 4
5. ############ ######### 5
6. ############# 8

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

(####), ### ######## # ###### ########### ###### ########## ######## ###4, ##### ######## ###### ###, ## ##### ######### ###### ########### # ##########, ### ########## #### ### #### ##### ######## ##. # ###### ######## ######### #### ########## ##–######## ############ ######## ######## ## ########## # # ##### ###########. #### ### ###### ########, ## ########### ######### ## ######### ###### ### ## ### ###–

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

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

2.

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

#####

Nie nale#y ########## ###### ### ########## #########: ###–######### # ######## # #### *wyklucza* ############ # #########. ##### ######## ######## ## ######## ######## # ##########.

###, ## ########### ############ ###### ###–#### ########## ######## ## ##### # ###### ############### ######## #### #####–###, ### # #########; ##### #### ######## ######## ######### ############## ### ######## #########. ## ######, ## ######### ##### #########, ######## ### ## ##### ### ########### ########### ##########. ## ###### ###### ##### ##### ######–###### ###, # ##### ##### 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. ######## ###### ######### #### ######–####### ########## ######## ##. ######### ## ############### ######### otwartego, ## ######### #### ######### #### ########## ########### (###### #### ####### ###### ##### ######## ########## # ######, ## #### ######### # #########, ### ############ ############## #### ####### ####). # ##### /etc/rc.conf ###### ####–#### ######## #####:

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

######## ###### ######## ############ ######### (######## #### ##### ipfw.ko, ##–### ### ###### ############ ## #####), # ###### ######### #### otwarty #### #### ##### (####### # ###### # /etc/rc.firewall). ######## ###### ######## ### ######### ##–######## #####, # # ######## ######## #### #############.

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

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

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

##########. ######## ### #### ########## ######### ##### # #########, #### ###### ### ###### ######## ########, ######### ######## ###### ####### # ###### otwartym, ### ############### ##########.

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

4. ############

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

```
# sysctl net.link.ether.bridge_cfg=fxp0:0,xl0:0
# sysctl net.link.ether.bridge_ipfw=1
# sysctl net.link.ether.bridge=1
```

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

###########. ##### ## ### #####–####, ##### ##### ## ##### /etc/sysctl.conf ##### net.link.ether.[co#]=[co#] ###### # ########–##, ## ####### ############ #### ######### #######.

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

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

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

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

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

#####

pe#n# ########, # ########## ##### #### ### ######## ##########, ## ##### ###### ######## ## #####.

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

```
# Szybkie przepuszczanie pakietów, których stan zosta# zapami#tany
add check-state

# Blokada sieci z 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

# Maszyna b#d#ca mostem mo#e wysy#a# co tylko zechce
# (je#li maszyna nie ma adresu IP, pomi# poni#sze wiersze)
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

# Stacje sieci wewn#trznej mog# wysy#a# co tylko zechc#
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

# Protokó# TCP
# Przepuszczanie SSH
add pass tcp from any to any 22 in via fxp0 setup keep-state
# Przepuszczanie SMTP jedynie do serwera poczty
add pass tcp from any to relay 25 in via fxp0 setup keep-state
# Informacje o obszarach mog# by# przesy#ane tylko przez podrz#dny
# serwer nazw [dns2.nic.it]
add pass tcp from 193.205.245.8 to ns 53 in via fxp0 setup keep-state
# Przepuszczanie zapyta# ident -- takie rozwi#zanie jest lepsze
# ni# oczekiwanie na przekroczenie czasu
add pass tcp from any to any 113 in via fxp0 setup keep-state
# Przepuszczenie zakresu portów dynamicznych
add pass tcp from any to any 49152-65535 in via fxp0 setup keep-state

# Protokó# UDP
# Przepuszczanie zapyta# DNS jedynie do serwera DNS
add pass udp from any to ns 53 in via fxp0 keep-state
# Przepuszczenie zakresu portów dynamicznych
add pass udp from any to any 49152-65535 in via fxp0 keep-state

# Protokó# ICMP
# Przepuszczanie -'pingów'
add pass icmp from any to any icmptypes 8 keep-state
# Przepuszczanie komunikatów o b##dach generowanych przez -'traceroute'
add pass icmp from any to any icmptypes 3
add pass icmp from any to any icmptypes 11

# Wszystko inne jest podejrzane
```

```
add drop log all from any to any
```

########## ###### ### ############# # ############ ######## #### ####### ###–## ## #### ####### ######. # #############, ####### ##### ############### ###–######## ###. ############, ##### ########## ##### *nie by#o* ######:

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

######## ### ########## ########, ##### ######### # ########, # #####, ## ## # ##### ###########. #### ## ###### ######### # #### ############## ### ##### ####### ############## ### ##### ###########, ############ ## ######### ###–####### ########, ############# ### ####### # ##### ###########. ###### # ###, ## #### *co najmniej* ##### ###### ######### # ########### ###########, ###### ### ##### ##########: #### ### #####. ###### ###### ####### ##### ############ ### ########### #### ##### ######## ##### ############# ## #### #######, ### ###### ### #### ### ##########.

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

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

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

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

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

6.

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

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

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