



```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεεᾶ οᾶβ÷ἰοο δñιόοᾶόβαο οἰῶ δῶñΠία.

**ΌγιαΒυός:** Άδου οι έαβιαί εαυηαβ υός Ύ÷ άαά άαάάάάάάάά άγι Ύέαιός 5.X οιό FreeBSD Ρ ιέα άεί άηυόάάό. Άί ÷ άγιόείάβία άγι Ύέαιός 4.X, ουόά έά άηΎάά ίά άίάηάίάίάάά άγι άάέίά Ρ *IPFW2* έάέ ίά άέάάΎάάά άγ άάβάά άίΡεάά ά *ipfw(8)* έάά άάέάάάάάάά άέάάάά άά ά άάέέΎ ίά άγι άάέίά Ρ *IPFW2*. άηίόΎάά έάάάάάάά άί άίάά *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFWALL_VERBOSE
```

ÓôÝéíáé ôá ìçíýíáôá ãéá ôá éáoÜëëçéá ðáéÝôá óôî log ôîõ óõóôÞíáôîð.

```
options IPFWERWALL_VERBOSE_LIMIT=500
```

[illegible]

```
options IPDIVERT
```

Áíãñäĩđĩéáß ôá *divert* sockets, ðĩõ èà äĩýĩà áñäüôãñá ôé êÛĩĩĩ.

[illegible]

3 ÅëéãÝò óôi /etc/rc.conf ãéá íá öĩñôþíáôáé ôĩ ôâß÷ìò  
ðñĩóôáóßàò

Ἄεά íá áíáñāīđīēáβōáé ôī ôāβ÷īō ðñīōōáōβāō éáōŬ ôçī áēēβīçōç ôīō ôōōōðīáōīō éáé áéá íá īñβōāōā ôī āñ÷āβī íā ôīōō éáíuíāō ôīō ôāβ÷īōō ðñīōōáōβāō, ðñŶđāé íá áīçīāñþróāō ôī āñ÷āβī /etc/rc.conf. ἌðēŬ ðñīōēŶōā ôēō ðāñāēŬōū āñāīŶð:

```
firewall_enable="YES"
firewall_script="/etc/firewall/fwrules"
```

Àéá ðàíéóóúðàñàò ðëçñröivñBåð ó-âðéêÛ iå ôç öçíáóBåð éåèäíéÛð áðu áððÝð èéð àñànÝð, ñBíðå íéå íáééÛ óðí /etc/default/rc.conf éåé äéääÛÓðå ôçí man óäèBää rc.conf(5)

## 4 ΆíññìðìéΠόοά όçí ΑίούìάòùìΎίç ìάòÛñάός Äéäðéýíóαùì όìò PPP

Άέά íά äðéòñÝðáòά óά Ûεéά ìç÷-áíΠíάóά όìò äééóýìò óάò íά óóíáÝìíóáé ìά όìì Ýìù éùóìì ìΎóù όìò FreeBSD, ÷ñçóéìðìéÞíóáò όì ùò “ðýèç”, éά ðñÝðáé íά áíñññìðìéΠόóáò όçí ΑίούìάòùìΎίç ìάòÛñάός äéäðéýíóαùì όìò PPP (NAT). Άέά íά áβíáé áòòù, ðñìóéÝóóά óòì áñ÷-áβì /etc/rc.conf óéò ðáñáéÛòù áñàììΎò:

```
ppp_enable="YES"
ppp_mode="auto"
ppp_nat="YES"
ppp_profile="ðñìòβë_ðçò_όγíäáόçò"
```

Όόç èΎόç όìò ðñìòβë\_ðçò\_όγíäáόçò ðñÝðáé íά áÛéäòά όì ùíñά óçò óýíäáóðò óάò, ùòòù όì Ύ÷-äòά áðìèçéäýóáé óòì áñ÷-áβì /etc/ppp/ppp.conf.

## 5 Ìé éáíüíäò όìò firewall

Όì ìüñ όìò áðñÝíáé ðÞñά áβíáé íά ìñβóìòìά όìòð éáíüíäò όìò firewall. Ìé éáíüíäò όìòð ìðìβìòð ðáñéáñÛóìòìά ääÞ áβíáé áñéäòÛ éáéìβ áéá όìòð ðáñéóóùòáñìòð ÷ñΠóóáò ìά dialup óýíäáόç, äééÛ ìýóά óðì÷-ñäùóééìβ áβíáé, ìýóά áβíáé äóíáòùì íά óáéñéÛæìòì ìά óéò áíÛäéäò ùéùì óùì ÷ñçóðÞ ìäíup. Ìðìñìýì, ùìòð, íά ÷ñçóéìäýóìòì ùò Ύíá éáéù ðáñÛäééäì ðòèìβóáùì όìò IPFW éáé áβíáé ó÷-äðééÛ äýéìèì íά όìòð ðñìóáñìüóáòά óóéò äééΎò óάò áíÛäéäò.

Áò áñ÷-βóìòìά ùìòð ìά óéò äáóééΎò áñ÷-Ύò áíüò éäééóóìý óáβ÷ìòð ðñìóóáóáò. Íá éäééóóù óáβ÷ìò ðñìóóáóáò ääáññäýáé éáò' áñ÷-Þì éÛéä óýíäáόç. Ì äéá÷-äéñéóóðò ìðìñáβ ýóóáñά íά ðñìóéÝóáé éáíüíäò äéá íά äðéòñÝðáé ìüñ óóäéäéñéìÝíäò óóíáÝóáéò íά ðáñìÛíá áðù όì óáβ÷ìò ðñìóóáóáò. Ç ðéì óðìçééóìΎίç óáéñÛ óùì éáíüíüí óά Ύíá éäééóóù óáβ÷ìò áβíáé: ðñÞóά ìé éáíüíäò όìò äðéòñÝðìòì ìáñééΎò óóíáÝóáéò, éáé óÝéìò ìé éáíüíäò όìò ääáññäýìòì ìðìéäáÞðìòά Ûéç óýíäáόç. Ç éñäéèÞ ðβóù áðù áòòù áβíáé ùóé ðñÞóά áÛæäòά όìòð éáíüíäò όìò äðéòñÝðìòì ðñÛäíáóά íά ðáñÛóìòì éáé ýóóáñά ùéá óά Ûεéá ääáññäýìíóáé áòòùìáóά.

ΌðéÛìòά, éìéðùì, Ύíá éáòÛéìäì óóìì ìðìβì éä áðìèçéäýìíóáé ìé éáíüíäò όìò óáβ÷ìòð ðñìóóáóáò. Óά áòòù όì Ûñéñì ÷ñçóéìðìéýìá ùò ðáñÛäééäì όìì éáòÛéìäì /etc/firewall. ΆééÛìòά éáòÛéìäì ìΎóά óά áòòùì éáé äçìéìòñáΠóóά όì áñ÷-áβì fwrules όìò όì ùíñÛ όìò áβ÷-äìá áñÛðáé óòì rc.conf. ΌçìäéÞóóά ðùò ìðìñáβóά íά äééÛìäòά όì ùíñά όìò áñ÷-áβìò áòòìý óά ùóé èΎéäòά. Áòòùò ì ìäçäùò áβíáé áòòù όì ùíñά óáí ðáñÛäééäì éáé ìüñ.

Áò äìýìá ðÞñά Ύíá ðáñÛäééäì óáβ÷ìòð ðñìóóáóáò ìά áñéäòÛ äðäìçäçìäóééÛ ó÷-ùééá.

```
# Define the firewall command (as in /etc/rc.firewall) for easy
# reference. Helps to make it easier to read.
fwcmd="/sbin/ipfw"
```

```
# Define our outside interface. With userland-ppp this
# defaults to tun0.
oif="tun0"
```

```
# Define our inside interface. This is usually your network
# card. Be sure to change this to match your own network
# interface.
iif="fxp0"
```

```
# Force a flushing of the current rules before we reload.
$fwcmd -f flush
```

```
# Divert all packets through the tunnel interface.
```

```
$fwcmd add divert natd all from any to any via tun0

# Check the state of all packets.
$fwcmd add check-state

# Stop spoofing on the outside interface.
$fwcmd add deny ip from any to any in via $oif not verrevpath

# Allow all connections that we initiate, and keep their state,
# but deny established connections that don't have a dynamic rule.
$fwcmd add allow ip from me to any out via $oif keep-state
$fwcmd add deny tcp from any to any established in via $oif

# Allow all connections within our network.
$fwcmd add allow ip from any to any via $iif

# Allow all local traffic.
$fwcmd add allow all from any to any via lo0
$fwcmd add deny all from any to 127.0.0.0/8
$fwcmd add deny ip from 127.0.0.0/8 to any

# Allow internet users to connect to the port 22 and 80.
# This example specifically allows connections to the sshd and a
# webserver.
$fwcmd add allow tcp from any to me dst-port 22,80 in via $oif setup keep-state

# Allow ICMP packets: remove type 8 if you don't want your host
# to be pingable.
$fwcmd add allow icmp from any to any via $oif icmp types 0,3,8,11,12

# Deny and log all the rest.
$fwcmd add deny log ip from any to any
```

Όπná Ý÷áoá Ýía ðēēçñüíÝíí óåβ÷ìò ðñüóóáóβáo, òì ïðßì óóíaÝóáéo óóéo èýñáo 22 éáé 80 éáé éáoáñÜöáé üēáo óéo Üēēáo óóíaÝóáéo óôi áñ÷åßì éáoáñáoðò òìò óóóðßáoìò. ÐēÝíí åβóóå Ýðēñē áéá åðáíæēßçóc. Ôì óåβ÷ìò ðñüóóáóβáo éå áíåññðēçēåß áóðüíáoá éáé éå òñòðóå òìò éáíüáo ðìò ðñüóēÝóáoå. Áí åå åßíæé áóðü Þ Ý÷áoå ïðēååððìò ðñüæßáoå, Þ áí Ý÷áoå èÜðēáo ðñüÜóáéo áéá íå áéññēèååß áóðü òì Üñēñì, åðēñēñüíßóóå íææ ïìò íå email.

## 6 ÅñüòÞóáéo

1. ÅēÝðü ìçíýíáoå üðüò limit 500 reached on entry 2800 éáé íåðÜ áðü áóðü òì óýóçìÜ ïì óóåíáoÜå íå éáoáñÜöáé óå ðåÝóå ðìò åñðñæñíóå áðü òì óåβ÷ìò ðñüóóáóβáo. Åñēåýåé áéñüå òì firewall ïìò;

Áóðü áðēÜ óçíåíå ðüò Ý÷æ ðñóéññðēçēåß òì ïÝæóòì ïñēñ éáoáñáoðò (logging) áéá áóðü òì éáíüå. Ì éáíüå ï ßæìò áíæññðēåß íå æñēåýåé, áēēÜ ååñ éå óóÝñíæ ðéå ìçíýíáoå óôi áñ÷åßì éáoáñáoðò òìò óóóðßáoìò ïÝ÷ñé íå ìçåñíóóå ðÜēé òìò ìåñçóÝò. Ìðñåßóå íå ìçåñíóóå òìò ìåñçóÝò ìå ççí áññēÞ

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðñáóáðá òì ùñéì éáóáññáðòðò óóέò ñðèìβóáέò òìò ððñáíá óáo ìá όçí áðέέìáÐ IPFWALL\_VERBOSE\_LIMIT ùðòð ðáñέáñÛðáìá ðáñáðÛñ. Ìðññáβóá íá áέέÛíáðá áðóó òì ùñéì (÷ ùñβò íá ìáðááèòóðβóáðá ðÛέέ òì ððñáíá óáo éάέ íá èÛíáðá reboot) ÷ ñçóέììðìέáíðáo όçí sysctl(8) όέìÐ net.inet.ip.fw.verbose\_limit.

2. ÈÛðìéì èÛèò ðñÝðáé íá Ýáέíá. Áέèìéçóá óέò áíòìéÝð éáoÛ ãñÛíá éάέ όþñá èèáέäþέçéá áðÝñ.

Áðóóò ì ìäçáùð òðìéÝðáé ùóέ ÷ ñçóέììðìέáβóá òì *userland-ppp*, áέ áðóó èέ ìé éáfííáð ðìò áβñíóáέ ÷ ñçóέììðìέíýì òì tun0 interface, ðìò áíóέóóìé÷ áβ óόçí ðñþόç óýíááόç ðìò óðέÛ÷ íáðáέ ìá òì ppp(8) (áέέέþð áñóóó èάέ ùð *user-ppp*). Ç áðñíáíç óýíááόç éá ÷ ñçóέììðìέíýóá òì tun1, ìáðÛ òì tun2 éάέ ðÛáέ èÝáñíóáð.

Èá ðñÝðáé áðβόçò íá èòìÛóðá ùóέ òì pppd(8) ÷ ñçóέììðìέáβ òì interface ppp0, ìðóðá áí ìáέέíáóáðá όç óýíááόÐ óáo ìá òì pppd(8) éá ðñÝðáé íá áíóέέáóáóóðáðá òì tun0 ìá ppp0. ÐáñáέÛóó èá ááβñíòìá Ýíá áýέèè ðñùðì íá áέέÛíáðá òìòò éáfííáð òìò firewall éáoðÛέέçéá. Ìé áñ÷έέìβ éáfííáð όþæííóáέ óá Ýíá áñ÷áβì ìá ùññá fwrules\_tun0.

```
% cd /etc/firewall
/etc/firewall% su
Password:
/etc/firewall# mv fwrules fwrules_tun0
/etc/firewall# cat fwrules_tun0 | sed s/tun0/ppp0/g > fwrules
```

Άέά íá éáóáέÛááðá áí ÷ ñçóέììðìέáβóá òì ppp(8) Ð òì pppd(8) ìðññáβóá íá áñáðÛóáðá όçí Ýññáì όçò ifconfig(8) áóìý áñáñáñðìέçéáβ ç óýíááόÐ óáo. Ð.÷., áέá ìéá óýíááόç ðìò áñáñáñðìέçéçéá áðó òì pppd(8) éá ááβðá èÛóέ óáf áðóó (ááβ÷ñíóáέ ìùì ìé ó÷áðέέÝð ãñáñìÝð):

```
% ifconfig
(skipped...)
ppp0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1524
    inet xxx.xxx.xxx.xxx --> xxx.xxx.xxx.xxx netmask 0xff000000
(skipped...)
```

Άðó όçí Ûέέç, áέá ìéá óýíááόç ðìò áñáñáñðìέçéçéá ìá òì ppp(8) (*user-ppp*) èÛ ðñáðá íá ááβðá èÛóέ ðáñññíéì ìá òì ðáñáέÛóó:

```
% ifconfig
(skipped...)
ppp0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
(skipped...)
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1524
    (IPv6 stuff skipped...)
    inet xxx.xxx.xxx.xxx --> xxx.xxx.xxx.xxx netmask 0xffffffff00
    Opened by PID xxxxx
(skipped...)
```