



```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεεᾶ οᾶβ÷ἰοο δñιόοᾶόβαο οἰῶ δῶñΠία.

**ΌγιαΒυός:** Άόου όι έαβιαί έαυηάβ υόε Ύ÷ άόά άαέάόάόόΡόάε όγι Ύέαιός 5.X όιό FreeBSD Ρ ιέα όεί όηύόόάός. Αί ÷ήόόείόίόιέαβόά όγι Ύέαιός 4.X, όυόά έα όηΎόάε ίά άίάηάίόίέΡόάόά όγι άόέέίΆΡ *IPFW2* έάέ ίά άέάάΎόάόά ός όάέβάά άίΡεάέό ipfw(8) έέά όαήέόόύόόαήάό όέόήίόίήβάό ό÷ άόέέΎ ίά όγι άόέέίΆΡ *IPFW2*. όήιόΎίόά έάέάβόάήά όι όίΡιά *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFWALL VERBOSE
```

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

```
options IPFIREWALL VERBOSE LIMIT=500
```

[illegible]

```
options IPDIVER
```

Āīāñāīōīēāβ ōā *divert* sockets, ðīō èā āīyīā āñāūōāñā ōē ēŪīīōī.

[illegible]

3 ÁëéãÑò óôi /etc/rc.conf ãéá íá öĩñôþíáôáé ôĩ ôâß÷ìò  
ðñĩóôáóþáò

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 áīçīāñþōáōā ôī āñ÷āβī /etc/rc.conf. ἌðēŬ ðñīōēŶōā ôēō ðāñāēŬōū āñāīŶð:

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

Άέά έάνέόόώδάνάό δέçñröivñßáó ó-άόέéŨ íà όç όçíáoßáó éáέáíéŨó áðü áòóŸó óέó άάáiŸó, ñßíôá íéá íáόéŨ óóí /etc/default/rc.conf éάé áéááŨóóá όçí man óάëßáá rc.conf(5)

4 ĀíāñāĩōĩēPóôā ôçí ĀíóùíáòùìÝíç İâôÜöñáóç Äéáõëýíóâuí ôĩõ PPP

[illegible]

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

Óðς εΥς οἷο δññòðð\_ðς\_óÝíááðς δñÝðáé íá àÙèàðà ðì úñíá ðςð óÝíááððð óáð, ùðùð ðì Ý÷áðá áððèçäýðáé ððì áñ÷áßì /etc/ppp/ppp.conf.

## 5 lé êáíüíàò ôïõ firewall

Òi iurì ðrò àðñÝíáε ððñá àβíáε íá ññβóíοíá ðíòð εáíuríáð ðíο firewall. Íε εáíuríáð ðíòð ðíβίβíòð ðñáεαñÙòíοíá áαð àβíáε áñεáðÙ εάεíβ áεά ðíòð ðñáεóóòðáñíòð ÷ ñβóðáð íá dialup óýíááóç, áεεÙ íýðá òðí÷ ÷ ñáòðεεíβ àβíáε, íýðá àβíáε áοíáðúí íá ðáεñεÙæíòí íá ðεð áíÙáεáð uεùí ðúí ÷ ñçóðí dialup. Ìðñíñí, uùð, íá ÷ ñçóéíáýòíòí uð Ýíá εáεù ðáñÙááεáíá ñòεíβóáúí ðíò IPFW εáε àβíáε ó÷ áòεεÙ áýεíεí íá ðíòð ðñíóáñíuóáðá óðεð áεéÝð óáð áíÙáεáð.

Ἄν ἀν÷Βοιτοῖα υἱὸς ἰὰ θεὸς ἀαεθεῖ Ὡς ἀν÷ Ὡς ἀφῦδ ἐεἰεοδίῳ ὁἶβ÷τὸδ ὁηιόδοἰοἶοἶο. ἰὰ ἐεἰεοδῦ ὁἶβ÷τὸ ὁηιόδοἰοἶοἶο  
 ἀδᾶαιηᾶγᾶε εἰο' ἀν÷βῖ εὔεα ὀγᾶἰο. Ἰ εἰα÷ἰεηεοἶοδῖο ἰθῖηᾶβ γόδοἰη ἰὰ ὁηιόε Ὡἰἰε εἰαφῦἰδ ἰεἰ ἰὰ ἀδεοἦ Ὡἰἰε ἰῦῖ  
 ὀἰεἰεηεἰῖ Ὡἰἰε ὀἰᾶ Ὡἰἰε ἰὰ ὁἰηῖ Ὡἰἰε ἀδῦ ὀῖ ὁἶβ÷τὸ ὁηιόδοἰοἶοἶο. ᾿ ᾿εῖ ὀῖῖεεοἰ Ὡἰῖ ὀἰηῖ ὀῖ εἰαφῦἰδ ὀἶ Ὡἰἰε  
 ἐεἰεοδῦ ὁἶβ÷τὸ ἀβῖἰε: ὁηῖοἶ ἰε εἰαφῦἰδ ὁῖο ἀδεοἦ Ὡἰἰε ἰᾶηεῖ Ὡἰἰε ὀἰᾶ Ὡἰἰε, εἰε ὀ Ὡἰἰε ἰε εἰαφῦἰδ ὁῖο ἀδᾶαιηᾶγᾶῖο  
 ἰῖῖεἰᾶβῖοἶο Ὡἰῖ ὀγᾶἰο. ᾿ εῖἰεῖ βῖοἶ ἀδῦ ἀοἶο ἀβῖἰε ὑἰε ὁηῖοἶ αὔᾶἰοἶ ὀῖοἶ εἰαφῦἰδ ὁῖο ἀδεοἦ Ὡἰἰε ὁηῖοἶ ὁηῖοἶ  
 ἰὰ ὁἰηῖ ὀῖῖ εἰε γόδοἰη ὑεἰ ὀἶ Ὡἰῖ ἀδᾶαιηᾶγᾶῖοἰε ἀοἶοἶοἶο.

Όσοι είναι, είδαμε, Υία εαδΰεταί οοί ιοίβι εα αδρεεαγίυοάε ιε εαφιαό οίο ααβ÷ιόο οηιόόαόβαιο. Οα αόοι οί ΰνεηι ÷ηόόεηιόηεγία υό δαηΰααεαία οίι εαδΰεταί /etc/firewall. Αεεΰιοά εαδΰεταί ιΰόα οά αόοιυ εαε αείειοηαόόα οί αη÷αβι fwrules δίο οί υμΰ οίο αβ÷αία αηΰόαε οόι rc.conf. Οείαεόόα δυό ιδηηάόα ία αεεΰιαόα οί υμια οίό αη÷αβίο αόοίυ οά υόε εΰεαόα. Αόουδ ι ιάαυό αβιαε αόοι οί υμια οάι δαηΰααεαία εαε ιυφι.

Áò àiŷià òpñá Ýiá ðãñŨäáéàìà ôâ÷ïòò ðñiíóôáóâáo ià áñêâòŨ äðâiçâçìàôéêŨ ó÷üëéá.

```
# 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 ìðìβì óðíaÝóáéo óóéo èýñáo 22 éáé 80 éáé éáoáñÜöáé üēáo óéo Üēēáo óðíaÝóáéo óôi áñ÷åβì éáoáñáoðò òìò óóóðìáoòìò. ÐēÝíí åβóðå Ýðìēñē áéá åðáíæēβìçóc. Ôì óåβ÷ìò ðñüóóáóβáo éå áíåññðìēçēåβ áóðüíáoá éáé éå òñòðóå òìò éáíüíáo ðìò ðñìóēÝóáoå. Áí åå åβíæé áóðü Þ Ý÷áoå ððìéååððìóå ðñìæðìáoå, Þ áí Ý÷áoå èÜðìéáo ðñìóÜóáéo áéá íå áéññēùēåβ áóðü òì Üñēñì, åðéēñēñìðóóå íææβ ììò íå email.

## 6 ÅñùòÞóáéo

1. ÅēÝðü ìçíýíáoå üðüò limit 500 reached on entry 2800 éáé íåóÜ áðü áóðü òì óýóóçìÜ ììò óðåíáoÜå íå éáoáñÜöáé óå ðåÝóå ðìò åìðñæñíóå áðü òì óåβ÷ìò ðñüóóáóβáo. Åìçåýåé áéñüå òì firewall ììò;

Áóðü áðēÜ óçíåβíæé ðüò Ý÷æ÷ñçóēñðìēçēåβ òì ìÝæóòì üñēñ éáoáñáoðò (logging) áéá áóðü òì éáíüíå. Ì éáíüíå ì Þæìò áíæññòēåβ íå æìçåýåé, áēēÜ ååñ éå óóÝñíæé ðéå ìçíýíáoå óôi áñ÷åβì éáoáñáoðò òìò óóóðìáoòìò ìÝ÷ñé íå ìçåñíóáoå ðÜçé òìò ìåññçóÝò. Ìðñåβóå íå ìçåñíóáoå òìò ìåññçóÝò ìå òçííñìð

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáßóá íá áóìßóáóá òì ùñéì éáóáññáößò óóéò ñöèìßóáέò òìò ðññßíá óáò ìá òçì áðéëíāß  
IPFWALL\_VERBOSE\_LIMIT ùðòò ðññéññÛðáì ðññáðÛñ. ìðññáßóá íá áέέÛíáóá áóóò òì ùñéì (÷ ùñßò íá  
ìáóáäèòóóßóáá ðÛέέ òì ðññßíá óáò éάέ íá èÛíáóá reboot) ÷ ñçóéììðéßíóáò òçì sysctl(8) óéìß  
net.inet.ip.fw.verbose\_limit.

2. ÈÛðéì èÛèò ðñÝðáé íá Ýáéíá. Áέëëýçóá óéò áíóëÝð éáóÛ ãñÛíá éάέ òþñá èéáéäþççá áðÝñ.

Áóóòò ì ìäçäòò òðñèÝðáé ùóé ÷ ñçóéììðééáßóá òì *userland-ppp*, áé áóóò èé ìé éáfííáð ðìò äßñíóáé ÷ ñçóéììðééíýì òì  
tun0 interface, ðìò áíóéóóé÷÷ äß óóçì ðñþòç óýíááóç ðìò óóéÛ÷ íáóáé ìá òì ppp(8) (áéçéþò áñóóò èάέ ùò *user-ppp*).  
Ç áðñíáíç óýíááóç éá ÷ ñçóéììðééíýóá òì tun1, ìáóÛ òì tun2 éάέ ðÛáé èÝñííóáð.

Èá ðñÝðáé áðßóçò íá èòìÛóóá ùóé òì pppd(8) ÷ ñçóéììðééáß òì interface ppp0, ìðòðá áí ìáééíßóáóá òç óýíááóß óáò ìá  
òì pppd(8) éá ðñÝðáé íá áíóééáóóóßóáóá òì tun0 ìá ppp0. ÐññáéÛòò éá äáßñíóíá Ýíá áýéëëì ðññðì íá áέέÛíáóá òìòò  
éáfííáð òìò firewall éáðÛέççá. ìé ãñ÷ééìß éáfííáð òþñííóáé óá Ýíá ãñ÷äßì 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
```

Άέá íá éáóáéÛááóá áí ÷ ñçóéììðééáßóá òì ppp(8) ð òì pppd(8) ìðññáßóá íá áíáðÛóáóá òçì Ýñíñì òçò ifconfig(8) áóñý  
áíñññðééççä ç óýíááóß óáò. Ð.÷., áέá ìéá óýíááóç ðìò áíñññðééçççä áðò òì pppd(8) éá äáßóá èÛóé óáf áóóò  
(äáß÷ñíóáé ìñì ìé ò÷äóééÝð ãñññÝð):

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

Άðò òçì Ûέçç, áέá ìéá óýíááóç ðìò áíñññðééçççä ìá òì ppp(8) (*user-ppp*) èÛ ðññðá íá äáßóá èÛóé ðññññéì ìá òì  
ðññáéÛòò:

```
% 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...)
```