


```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεεᾶ οᾶβ÷ἰοο θῆιόοᾶόβαο οἰῶ θῶῆΠία.

ΌγιαΒυός: Άδου οι έαβιαί έαυηάβ υός Ύ÷ άόά άάέάόάόΠόάέ όγι Ύέαιός 5.X οιό FreeBSD Π ιέα όεί όηύόόάό. Αί ÷ήόόείόίόιέαβόά όγι Ύέαιός 4.X, όύόά έά όηΎόάέ ίά άίάηάίόίέΠόάόά όγι άόέέϊΑΠ *IPFW2* έάέ ίά άέάάΎόάόά ός όάέβάά άίΠεάέό ipfw(8) έέά όηέόόόύόόηάό όέόηίόίηβάό ό÷ άόέέΎ ίά όγι άόέέϊΑΠ *IPFW2*. ΌηίόΎίόά έάέάβόάηά όί όίΠιά *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFWALL VERBOSE
```

ÓôÝéíáé ôá ìçíýíáôá äéá ôá éáoÜëëçéá ðáéÝôá óôî log ôîõ óõóóÞíáôîð.

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

[illegible]

```
options IPDIVER
```

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

[illegible]

3 ÁëéãÿÒ óôï /etc/rc.conf ãéá íá öïñôþíáôáé ôï ôâß÷ìò
ðñïóôáóßàò

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

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

Àéá ðáñéóóúóáñáó ðéçñíóíñBáó ó-áóééÜ íà ðç óçíáóBáó éáéáñéÜó áóü áóóÝó óéó áñáñÝó, ñBíóá íéá íáóéÜ óóí /etc/defaults/rc.conf éáé áéááÜóóá óçí man óáéBáá rc.conf(5)

4 ΆíññìðìéΠóóå ôçí ΆíóùìáòùìΎìç ìåðÛññåç Äéåðëýíóåùì òìò PPP

Άέά íå äðéòñÝðååå óå Ûëëå ìç÷årìååå òìò åééðýìò óåå íå óðíåÝìíóåé ìå òìì Ýìù èùòìì ìΎóù òìò FreeBSD, ÷ñçóëìðìéðìååå òì ùð “ðýëç”, åå ðñÝðåé íå åíññìðìéΠóóåå ôçí åíóùìáòùìΎìç ìåðÛññåç äéåðëýíóåùì òìò PPP (NAT). Άέå íå åßíåé åðòù, ðñìéÝóååå óðì åñ÷åßì /etc/rc.conf ðéð ðåñåÛòù åñåñìÝð:

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

Όçç èΎóç òìò ðñìðßë_ðçð_όγιάååçð ðñÝðåé íå åÛëååå òì ùñåå ççð óýìåååðð óåð, ùðòò òì Ύ÷ååå äðìçëåýóåé óðì åñ÷åßì /etc/ppp/ppp.conf.

5 Ìé éåíüìåò òìò firewall

Όì ìñì ðìò äðñìÝíåé ðññå åßíåé íå ìñßòìåå òìòð éåñìåå òìò firewall. Ìé éåñìåå òìòð ìðìßìòð ðåñéåñÛòìòìåå ååð åßíåé åñëåðÛ éåñìß åéå òìòð ðåñéóóùðåñìòð ÷ñΠóóåå ìå ðìååç óýìååç, åëëÛ ìýåå òðì÷ñåðéëß åßíåé, ìýåå åßíåé åðíååùì íå óåññÛåñìòì ìå ðéð åñÛååå ùëùì òùì ÷ñçóððì ðìååç. ÌðñìÝì, ùìò, íå ÷ñçóëìåýóòìòì ùð Ύíå éåëù ðåñÛåååñìå ðñëìßååùì òìò IPFW éåé åßíåé ó÷åðéëÛ åýëìì íå òìòð ðñìóåñìùóååå óðéð åéëÝð óåð åñÛååå.

Áð åñ÷åðìåå ùìò ìå ðéð ååóéëÝð åñ÷Ýð åñùð èëåéóòìý ðåß÷ìòð ðñìóóåååå. ìå èëåéóòù ðåß÷ìòð ðñìóóååååå äååññåýåé éåð’ åñ÷Πì èÛëå óýìååç. Ì åéå÷åñéóóðð ìðññåß ýóóåñå íå ðñìéÝóåé éåñìåå åéå íå äðéòñÝðåé ìñì óðåååññéÝíåå óðíåÝóåé ìå ðåñìÛíå åðù òì ðåß÷ìòð ðñìóóåååå. Ç ðéì óðìçëéóìΎìç óåññÛ òùì éåñìåå óå Ύíå èëåéóòù ðåß÷ìòð åßíåé: ðñðåé ìé éåñìåå ðìò äðéòñÝðìòì ìåñéëÝð óðíåÝóåé, éåé ðÝëìò ìé éåñìåå ðìò äðåññåýìòì ìðìåååððìåå Ûëçç óýìååç. Ç ëñåçëΠ ðßòù åðù åðòù åßíåé ùéé ðñðåé åÛåååå òìòð éåñìåå ðìò äðéòñÝðìòì ðñÛåíååå íå ðåñÛòìòì éåé ýóóåñå ùëå óå Ûëëå äðåññåýìíóåé åðòùìååå.

ΌðéÛìåå, ëñðùì, Ύíå éåðÛëñåì óðì ìðìßì éå äðìçëåýìíóåé ìé éåñìåå òìò ðåß÷ìòð ðñìóóåååå. Όå åðòù òì Ûñëñì ÷ñçóëìðìéýìåå ùð ðåñÛåååñìå òì éåðÛëñåì /etc/firewall. ΆëëÛìåå éåðÛëñåì ìΎóå óå åðòùì éåé åçìéìðñåΠóóåå òì åñ÷åßì fwrules ðìò òì ùñìÛ òìò åß÷ååå åñÛåé óðì rc.conf. Όçìåçðóåå ðùð ìðññåååå íå åëëÛååå òì ùñåå òìò åñ÷åßì åðòìý óå ùéé èΎëååå. Άðòùð ì ìåçåð åßíåé åðòù òì ùñåå óåñ ðåñÛåååñìå éåé ìñì.

Áð åñýìå ðññå Ύíå ðåñÛåååñìå ðåß÷ìòð ðñìóóååååå ìå åñëåðÛ äðåñçåçìåéëÛ ó÷åëåå.

```
# 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 icmptypes 0,3,8,11,12

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

Όþñá Ý÷áoά Ýία ðεìεεçñüìÝíí óαβ÷ιò ðñüóóáóβáo, òì ìðìβì óðíáÝóáέò óóέò εýñáo 22 έάέ 80 έάέ έáoáñÜöάέ üεáo óέò Üεέáo óðíáÝóáέò óôi άñ÷άβì έáoáññáoðò òìò óóóðßíáoìò. ÐεÝíí άβóóά Ýðìεííε άέά άðáíάέεβίçóç. Όì óαβ÷ιò ðñüóóáóβáo έά άíáñáðìεçεάβ άóòüíáoά έάέ έά öìòðóάε òìò έáíüíáo ðìò ðñìóεÝóáoά. Áí άά άβíάέ άóòü Þ Ý÷áoά ðìεάáððìóά ðñíάεßíáoά, Þ άí Ý÷áoά εÜðìεáo ðñìóÜóáέò άέά íá άέíñεùεάβ άóòü òì Üñεñì, άðέεíεíüíßóóά íάεβ ììò íá email.

6 Άñüòßóáέò

1. ΆεÝðü ìçíýíáoά üðüò “limit 500 reached on entry 2800” έάέ íáoÜ áðü άóòü òì óýóòçìÜ ììò óóáíáoÜάέ íá έáoáññÜöάέ óá ðάεÝóά ðìò άìðíáβæííóάέ áðü òì óαβ÷ιò ðñüóóáóβáo. Άìòεáýάέ άέüíá òì firewall ììò;

Άóòü άðεÜ óçíáβíάέ ðüò Ý÷άε ðñçóéíìðìεçεάβ òì ìÝάέóòì üñέí έáoáññáoðò (logging) άέά άóòü òì έáíüíá. Ì έáíüíáo ì βάέìò άíάεíεíòεάβ íá äìòεáýάέ, άέεÜ ááí έά óóÝεíάέ ðéá ìçíýíáoά óôi άñ÷άβì έáoáññáoðò òìò óóóðßíáoìò ìÝ÷ñέ íá ìçáíßóáoά ðÜέέ òìò ìáoñçòÝò. Ìðñíáβóά íá ìçáíßóáoά òìò ìáoñçòÝò ìά òçí áíòìεÞ

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðñáóáðá òñ ùñéñ éáóáññáöðò óóέò ñòèìβóáέò òñ ððñá íá óáo ìá òçñ áðéññá IPFWALL_VERBOSE_LIMIT ùðò ðáñéññÛðáì ðáñáðÛñ. Ìðññáβóá íá áέέÛíáðá áðóó òñ ùñéñ (÷ ùñβò íá ìáðááèòóóβóáðá ðÛέέ òñ ððñá íá óáo éάέ íá èÛíáðá reboot) ÷ ñçóéññðéñíðáo òçñ sysctl(8) óéì net.inet.ip.fw.verbose_limit.

2. ÈÛðñéñ èÛèò ðñÝðáé íá Ýáéíá. Áέñéýçóá óέò áñòñÝð éáoÛ ãñÛíá éάέ òþñá èéáéäþçéá áðÝñ.

Áðóóò ì ìäçáùð òðñéÝðáé ùðé ÷ ñçóéññðéñáβóá òñ *userland-ppp*, áé áðóó èé ìé éáfñíáð ðñ ãβññóáé ÷ ñçóéññðéñíýñ òñ tun0 interface, ðñ áíóέóðñé÷ áβ óðçñ ðñþðç óýíááóç ðñ òðéÛ÷ íáðáé ìá òñ ppp(8) (áέέþð ãñóóó èάέ ùð *user-ppp*). Ç áðñíáç óýíááóç éá ÷ ñçóéññðéñíýóá òñ tun1, ìáðÛ òñ tun2 éάέ ðÛáé èÝáññóáo.

Èá ðñÝðáé áðβóçò íá èòìÛóðá ùðé òñ pppd(8) ÷ ñçóéññðéñáβ òñ interface ppp0, ìðóðá áñ ìáέéñáóáðá òç óýíááóð óáo ìá òñ pppd(8) éá ðñÝðáé íá áíóέéáóóðáóðá òñ tun0 ìá ppp0. ÐáñáéÛóó èá ãáβññóíá Ýíá áýéññ ðññðñ íá áέéÛíáðá òñ òð éáfñíáð òñ firewall éáoðÛέçéá. Ìé áñ÷ééñβ éáfñíáð òþññíóáé óá Ýíá áñ÷áβ 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 éáðáéÛááðá áñ ÷ ñçóéññðéñáβðá òñ ppp(8) Ð òñ pppd(8) ìðññáβóá íá áñáðÛóáðá òçñ Ýñññ òçð ifconfig(8) áóñý áññññðñéçéáβ ç óýíááóð óáo. Ð.÷., áέá ìéá óýíááóç ðñ áññññðñéçéçéá áðñ òñ pppd(8) éá ãáβðá èÛóé óáí áðóó (ãáβ÷ññóáé ìññ ìé ò÷áðééÝð ãñññÝð):

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

Áðñ òçñ Ûέçç, áέá ìéá óýíááóç ðñ áññññðñéçéçéá ìá òñ ppp(8) (*user-ppp*) èÛ ðññðá íá ãáβðá èÛóé ðáññññéñ ìá òñ ðáñáéÛóó:

```
% 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 0xffffffff
    Opened by PID xxxxx
(skipped...)
```