


```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεεᾶ οᾶβ÷ἰοο δñιόοᾶόβαο οἰῶ δῶñΠία.

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

```
options IPFWALL VERBOSE
```

ÓôÝéíáé ôá ìçíýíáôá ãéá ôá éáoÜëëçéá ðáéÝôá óôi log ôiõ óõóôÞíáôîò.

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

[illegible]

```
options IPDIVERT
```

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

[illegible]

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

Ἄεά íá áíáñāīđīēáβōáé ôī ôāβ÷īō ðñīōōáōβáō éáōŨ ôçī áēēβīçōç ôīō ôōōōðīáōīō éáé áéá íá īñβōáōā ôī āñ÷āβī íā ôīōō éáíuíāō ôīō ôāβ÷īōō ðñīōōáōβáō, ðñŸđāé íá áīçīāñþróāō ôī āñ÷āβī /etc/rc.conf. ÁðēŨ ðñīōēŸōā ôēō ðāñāēŨōū āñāīŸō:

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

```
Ääå ðänëööüöñâño ðeçñröinBão ö-äöéÜ íà õç óçíáóBáo éäéäñéÜð äðu äðöÝð öéo añanìÝð, nBíõä íéä íäöéÜ öði  
/etc/default/rc.conf éäé äéääÜöðä öçí man öäèßää rc.conf(5)
```

4 ΆíññìðìéΠóóå ôçí ΆíóùìáòùìΎìç ìåðÛññåç Äéåðëýíóåùì òìò PPP

Άέά íå äðéòñÝðååå óå Ûëëå ìç÷åíìååå òìò äééðýìò óåå íå óðíåÝìíóåé ìå òìì Ýìù èùòì ìΎóù òìò FreeBSD, ÷ñçóëìðìéðìååå òì ùð “ðýëç”, åå ðñÝðåé íå áíñññìðìéΠóóåå ôçí άíóùìáòùìΎìç ìåðÛññåç äéåðëýíóåùì òìò PPP (NAT). Άέå íå åβíåé åðòù, ðñìéÝóåå óòì åñ÷åíìåå /etc/rc.conf ðéð ðåñåÛòù åñåñìÝð:

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

Όόç èΎóç òìò ðñìððë_ðçð_όγιάαός ðñÝðåé íå åÛëååå òì ùñåå ðçð óýìååðð ðåð, ùðòò òì Ύ÷ååå äðìçëåýóåé óòì åñ÷åíìåå /etc/ppp/ppp.conf.

5 Ìé éåíüìåò òìò firewall

Όì ìññì ðìò äðñìÝíåé ðññå åβíåé íå ìñβóìñå òìò éåññåå òìò firewall. Ìé éåññåå òìò ìðìβìòð ðåñåñÛòìñå ååð åβíåé åñëåðÛ éåññ åéå òìòð ðåñåóóùðåññìòð ÷ñΠóóåå ìå dialup óýìååç, äéëÛ ìýåå òðì÷ñåðéñ åβíåé, ìýåå åβíåé äðñååùì íå óåññÛåññìò ìå ðéð åñÛååð ùëù òùì ÷ñçóððì dialup. Ìðññìýì, ùìò, íå ÷ñçóëìåýóòì ùð Ύíå éåëù ðåñÛåååñå ðñëìβååùì òìò IPFW éåé åβíåé ó÷åðéëÛ åýëññ íå òìòð ðñìóåñññóååå óééð äéëÝð óåå åñÛååð.

Áð åñ÷åíìåå ùìò ìå ðéð ååóéëÝð åñ÷Ýð åññð èëåóóòý ðåβ÷ìòð ðñìóóåååå. ìå èëåóóòù ðåβ÷ìòð ðñìóóååååå äðåññåñåé ååð’ åñ÷Πì èÛëå óýìååç. Ì åéå÷åñéóóðð ìðññåé ýóóåñå íå ðñìéÝóåé éåññåå åéå íå äðéòñÝðåé ìññì óóåååñññìÝíåå óðñåÝóåé ìå ðåññÛíå äðù òì ðåβ÷ìòð ðñìóóåååå. Ç ðéì óðìçééóìΎìç óåññÛ òùì éåññññ ðå Ύíå èëåóóòù ðåβ÷ìòð åβíåé: ðñðåé ìé éåññåå ðìò äðéòñÝðìò ìåñéëÝð óðñåÝóåé, éåé ðÝëìò ìé éåññåå ðìò äðåññåñññìò ìðñååððìåå Ûëçç óýìååç. Ç ëñåçëΠ ðβòù äðù åðòù åβíåé ùéé ðñðåå åÛåååå òìòð éåññåå ðìò äðéòñÝðìò ðñÛåñåå íå ðåñÛòìò éåé ýóóåñå ùëå ðå Ûëëå äðåññåññññåé åðòùìåå.

ΌéëÛìå, ëñðññ, Ύíå éåðÛëññ óòì ìðìβì éå äðìçëåýñññåé ìé éåññåå òìò ðåβ÷ìòð ðñìóóåååå. Όå åðòù òì Ûñëññ ÷ñçóëìðìéýññ ùð ðåñÛåååñå òì éåðÛëññ /etc/firewall. ΆéëÛìå éåðÛëññ ìΎóå óå åðòù éåé åçìéìñåΠóóåå òì åñ÷åíìåå ðìò òì ùññÛ òìò åβ÷åñå åñÛåé óòì rc.conf. Όçñåéðåå ðùð ìðññååå íå äéëÛååå òì ùññå òìò åñ÷åíìåå åðòý óå ùéé èΎëåå. Áðòùð ì ìåçåð åβíåé åðòù òì ùññå óåñ ðåñÛåååñå éåé ìññ.

Áð åñññå ðññå Ύíå ðåñÛåååñå ðåβ÷ìòð ðñìóóååååå ìå åñëåðÛ äðåñçåñåéëÛ ó÷åëå.

```
# 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
```

Όþñá Ý÷áðá Ýíá ðñüóóáóßáò, òì ìðñì óðíáÝóáéò óðéò èýñáò 22 éáé 80 éáé éáðáñÜöáé üéáò óéò Üééáò óðíáÝóáéò óõï áñ÷áßì éáðáñáðò òìò óðóðßíáòì. ÐéÝì áßóðá Ýðñéñé áéá áðáíáéßíçòç. Ôì ðåβ÷ìò ðñüóóáóßáò éá áíáñáðñéçéåß áðóñíáðá éáé éá òñòðóáé òìò éáñíáð ðìò ðñüéÝóáðá. Áí áá áßíáé áðóð ð Ý÷áðá ðñééáððñíá ðñíáéßíáð, ð áí Ý÷áðá èÜðñéáð ðñüóóáéò áéá íá áéññéðéåß áðóð òì Üñèñì, áðéçñéñíðóðá íáæß ììò íá email.

6 ÄñùòÞóáéò

1. ÄéÝðñ ìçíýíáðá üðñò “limit 500 reached on entry 2800” éáé íáðÜ áðñ áðóð òì óýóðçìÜ ììò óðáíáðÜáé íá éáðáñÜöáé ðá ðáéÝóá ðìò áìðñáæñíðáé áðñ òì ðåβ÷ìò ðñüóóáóßáò. Äìðéáýáé áéñíá òì firewall ììò;

Áðóð áðéÜ óçíáßíáé ðñò Ý÷áé ðñóéñìðñéçéåß òì ìÝáéóòì ùñéì éáðáñáðò (logging) áéá áðóð òì éáñíá. Ì éáñíáð ì ðáéì áíáçññéðéåß íá áñéçáýáé, áééÜ ááí éá óóÝçíáé ðéá ìçíýíáðá óõï áñ÷áßì éáðáñáðò òìò óðóðßíáòì ìÝ÷ñé íá ìçáñíáðáðá ðÜéé òìò ìáðñçðÝð. Ìðñíáßðá íá ìçáñíáðáðá òìò ìáðñçðÝð ìá òçí áññéð

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðñáóáðá òì ùñέì éάόάññáðòðò óóέò ñðèìβóάέò òìò ððñá íá óáo ìá όçí áðέέìáÐ IPFWALL_VERBOSE_LIMIT ùðòð ðáñέáñÛðáì ðáñáðÛñ. Ìðññáβóá íá áέέÛíáðá áðóó òì ùñέì (÷ ùñβò íá ìáðááèòóðβóáðá ðÛέέ òì ððñá íá óáo éάέ íá èÛíáðá reboot) ÷ ñçóέììðìέáðáð όçí sysctl(8) όέìÐ net.inet.ip.fw.verbose_limit.

2. ÈÛðìέì èÛèò ðñÝðáέ íá Ýáέíá. Áέèìýçóá óέò áíòìÝð éáoÛ ãñÛíá éάέ όþñá èèáέäþèçéá áðÝñ.

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

Èá ðñÝðáέ áðβόçò íá èòìÛóðá ùðέ òì pppd(8) ÷ ñçóέììðìέáβ òì interface ppp0, ìðóðá áí ìáέέíáóáðá όç óýíááόÐ óáo ìá òì pppd(8) éá ðñÝðáέ íá áíóέéάóáóðβóáðá òì tun0 ìá ppp0. ÐáñáέÛóó èá ááβñíòìá Ýíá áýέèì ðñùðì íá áέέÛíáðá òìòò éáfííáð òìò firewall éάðÛέçéá. Ìέ 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 éάóáέÛááðá áí ÷ ñçóέììðìέáβóá òì ppp(8) Ð òì pppd(8) ìðññáβóá íá áñáðÛóáðá όçí Ýññáì όçò ifconfig(8) áóìý áñáñáñðìέçéáβ ç óýíááόÐ óáo. Ð.÷., áέá ìέá óýíááόç ðìò áñáñáñðìέçéçéá áðó òì pppd(8) éá ááβðá èÛóέ óáf áðóó (ááβ÷ñíóáέ ìùì ìέ 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 Ûέçç, áέá ìέá óýíááόç ðìò áñáñáñðìέçéçéá ìá òì ppp(8) (*user-ppp*) èÛ ðñáðá íá ááβðá èÛóέ ðáñññìέì 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...)
```