


```
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 άόέέϊΑΠ *IPFW2* έάέ ίά άέάάΎόάόά όγ όάέβάά άίΠεάέό ipfw(8) έέά όηέόόόύόάηάό όέγνιόιηβάό ό÷ άόέέΎ ίά όγι άόέέϊΑΠ *IPFW2*. ΠηιόΎίόά έάέάβόάηά όι όίΠιά *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFWALL VERBOSE
```

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

```
options IPFWIREWALL 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"
```

Àéá ðàíéóóúðàñàò ðëçñröivñBäò ó-äòéèÛ iä ôç öçíáóBäò éäéäíéÙò äðu äòðÝò èéð àñànÝò, ñBíôä íéä íáééÛ öði /etc/default/rc.conf éäé äéääÛöðä öçí man óäëBää rc.conf(5)

4 ΆíññìðìέΠóòά όçí ΑίóύìáòùìΎίç ìáòÛññάόç Äέáðēýíóáùì óìò PPP

Άέά íá äðέòñÝðáòá óá Ûέέá ìç÷áíΠíáóá òìò äέέóýìò óáò íá óòíáÝìíóáέ ìá òìí Ύìù èùòì ìΎóù òìò FreeBSD, ÷ñçóέììðìέΠíóáò òì ùò “ðýέç”, έá ðñÝðáέ íá áíñññìðìέΠóòáò όçí ΑίóύìáòùìΎίç ìáòÛññάόç äέáðēýíóáùì òìò PPP (NAT). Άέά íá áβíáέ áòòù, ðñìóέΎóáò óòì áñ÷áβì /etc/rc.conf óέò ðáñáέÛòù áñáñΎò:

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

Όόç èΎόç òìò ðñìòβέ_òçò_όγíááόçò ðñÝðáέ íá áÛέáòá òì ùíñá όçò όγíááόçò óáò, ùòòù òì Ύ÷áòá áðìέçέáýóáέ óòì áñ÷áβì /etc/ppp/ppp.conf.

5 Ìέ έáíüíáò òìò firewall

Όì ìüñ ðìò áðñΎíáέ òðñá áβíáέ íá ìñβóìòìá òìò έáíüíáò òìò firewall. Ìέ έáíüíáò òìò ìðìβìòð ðáñέáñÛòìòìá ááð áβíáέ áñέáòÛ έáέìβ áέá òìòð ðáñέóóùòáñìòð ÷ñΠóóáò ìá dialup όγíááόç, áέέÛ ìýóá òðì÷ñáùóέέìβ áβíáέ, ìýóá áβíáέ áòíáòùì íá óáέñέÛέìòì ìá óέò áíÛáέáò ùέùì òùì ÷ñçóòðì dialup. Ìðìñìýì, ùìò, íá ÷ñçóέìáýóòìò ùò Ύíá έáέù ðáñÛáέέìá ðòèìβóáùì òìò IPFW έáέ áβíáέ ó÷áðέέÛ áýέìì íá òìòð ðñìóáñìüóáòá óóέò áέέΎò óáò áíÛáέáò.

Áò áñ÷βóìòìá ùìò ìá óέò ááóέέΎò áñ÷Ύò áíüò èέáέóòìý óáβ÷ìòð ðñìóóáóáò. ðá èέáέóóù óáβ÷ìò ðñìóóáóáò áðááññáýáέ έáò’ áñ÷Πì έÛέá όγíááόç. Ì áέá÷áέñέóóð ìðìñáβ ýóóáñá íá ðñìóέΎóáέ έáíüíáò áέá íá äðέòñÝðáέ ìüñ óóáέáèñέΎíáò óòíáΎóáέò íá ðáñìÛíá áðù òì óáβ÷ìò ðñìóóáóáò. Ç ðέì óòìçέέòìΎίç óáέñÛ òùì έáíüíüí óá Ύíá èέáέóóù óáβ÷ìò áβíáέ: ðñðóá ìέ έáíüíáò ðìò äðέòñÝðìòì ìáñέέΎò óòíáΎóáέò, έáέ òΎέìò ìέ έáíüíáò ðìò áðááññáýìòì ìðìέááΠðìòá Ûέέç όγíááόç. Ç έìáέέΠ ðβóù áðù áòòù áβíáέ ùóέ ðñðóá áÛέáòá òìòð έáíüíáò ðìò äðέòñÝðìòì ðñÛáíáóá íá ðáñÛóìòì έáέ ýóóáñá ùέá óá Ûέέá áðááññáýìíóáέ áòòùìáóá.

ΌðέÛìòá, έìέðùì, Ύíá έáòÛέìáì óòì ìðìβì έá áðìέçέáýìíóáέ ìέ έáíüíáò òìò óáβ÷ìòð ðñìóóáóáò. Όá áòòù òì Ûñèñì ÷ñçóέììðìέìýìá ùò ðáñÛáέέìá òì έáòÛέìáì /etc/firewall. ΆέέÛìòá έáòÛέìáì ìΎóá óá áòòùì έáέ äçìέìòñáΠóóá òì áñ÷áβì fwrules ðìò òì ùíñÛ òìò áβ÷áì áñÛáέ óòì rc.conf. ΌçìáέΠóóá ðùò ìðìñáβóá íá áέέÛíáòá òì ùíñá òìò áñ÷áβìò áòòìý óá ùóέ èΎέáòá. Áòòùò ì ìáçáùò áβíáέ áòòù òì ùíñá óáí ðáñÛáέέìá έáέ ìüñ.

Áò áñýìá òðñá Ύíá ðáñÛáέέìá óáβ÷ìòð ðñìóóáóáò ìá áñέáòÛ áðáñçáçìáðέέÛ ó÷έέá.

```
# 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÷áoά Ύía ðèèçñüìÝíí óåβ÷ìð ðñüóóáóβáo, òì ìðìβì óðíaÝóáέð óðέð èýñåð 22 έάέ 80 έάέ έáoåñÜöåέ üèåð óέð Üèèåð óðiaÝóáέð óôi åñ÷åβì έáoåñåöðð òìð óóóðßiaðìð. ÐèÝíí åβóðå Ύðìèíè έέå åðáíåèèβίçç. Όì óåβ÷ìð ðñüóóáóβáo έå áíåñåðìèçέåß áððüìiaóå έάέ έå òìððóåέ òìðð έáíüíåð ðìð ðñìóèÝóáóå. Áí åå åβíåέ áððü ð Ý÷áoå ððìέååððìåð ðñíåèßiaóå, ð áí Ý÷áoå èÜðìέåð ðñìóÜóáέð åέå íå έέíñèèèååß áððü òì Üñèñí, åðέèìèíüßóóå íåèß ìðò íå email.

6 Åñüòßóåέð

1. ÅèÝðñü ìçíýiaóå üðñð “limit 500 reached on entry 2800” έάέ íåðÜ áðñü áððü òì óýóðçìÜ ìð óðáíåðÜåέ íå έáoåñåÜöåέ óå ðåèÝóå ðìð åìðñåèííåðåέ áðñü òì óåβ÷ìð ðñüóóáóβáo. Åìèèåýåέ åèñüð òì firewall ìð;

Áððü áðèÜ óçíåèíåðð ðñð Ý÷å ðñçóèííèçέåß òì ìÝåóðì ìñèí έáoåñåöðð (logging) åέå áððü òì έáíüíå. Ì έáíüíåð ì Òåèð áíåèìèðèåß íå åìèèåýåέ, åèèÜ åå έå óðÝèíåέ ðåå ìçíýiaóå óôi åñ÷åβì έáoåñåöðð òìð óóóðßiaðìð ìÝ÷ñé íå íå íçåñíåðåð ðÜèè òìðò íåðñçðÝð. Ìðñíåèå íå íçåñíåðåð òìðò íåðñçðÝð ìå òçí áíèèèð

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáßóá íá áðìßóáóá òì ùñέì éάόάññáößò óóέò ñòèìßóáέò òìò ðòñßíá óάò ìá όçí áðέέìāß IPFWALL_VERBOSE_LIMIT ùðòò ðññέññÛðáìá ðññáðÛñ. ìðññáßóá íá áέέÛíáóá áóóò òì ùñέì (÷ ùñßò íá ìáóáäèòóóßóáá ðÛέέ òì ðòñßíá óάò éάέ íá èÛíáóá reboot) ÷ ñçóέììðìέßíóáò όçí sysctl(8) όέìß net.inet.ip.fw.verbose_limit.

2. ÈÛðìέì èÛèò ðñÝðáέ íá Ýáέíá. Áέèìέçóá óέò áíòìέÝò éάóÛ ãñÛìá éάέ όþñá èèáέäþέçéá áðÝñ.

Áóóòò ì ìāçāùò òðìέÝðáέ ùóέ ÷ ñçóέììðìέáßóá òì *userland-ppp*, áέ áóóò èέ ìέ éáfñíáð ðìò äßñíóáέ ÷ ñçóέììðìέíýì òì tun0 interface, ðìò áíóέóóìέ÷ äß óόçì ðñþόç óýíááόç ðìò óóέÛ÷ íáóáέ ìá òì ppp(8) (áέέέþò áñóóò èάέ ùò *user-ppp*). Ç áðñíáç óýíááόç éá ÷ ñçóέììðìέíýóá òì tun1, ìáóÛ òì tun2 éάέ ðÛáέ èÝññíóáò.

Èá ðñÝðáέ áðßόçò íá èòìÛóóá ùóέ òì pppd(8) ÷ ñçóέììðìέáß òì interface ppp0, ìðòá áí ìáέέìßóáóá όç óýíááόß óάò ìá òì pppd(8) éá ðñÝðáέ íá áíóέéάóáóóßóáá òì tun0 ìá ppp0. ÐññáέÛóò éá ääßñíóìá Ýíá áýέèì ðññðì íá áέέÛíáóá òìòò éáfñíáð òìò firewall éάóÛέέçéá. ìέ ãñ÷έέìß éáfñíáð όþññíóáέ óá Ýíá ãñ÷áßì 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 éάóáέÛááóá áí ÷ ñçóέììðìέáßóá òì ppp(8) ð òì pppd(8) ìðññáßóá íá áñáóÛóáóá όçì Ýñññì όçò ifconfig(8) áóìý áññññðìέçéäß ç óýíááόß óάò. Ð.÷., áέá ìέá óýíááόç ðìò áññññðìέçéçéá áðñ òì pppd(8) éá ääßóá èÛóέ óáf áóóò (ääß÷ññóáέ ìñì ìέ ó÷äóέέÝò ãñññìÝò):

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

Άðñ όçì Ûέέç, áέá ìέá óýíááόç ðìò áññññðìέçéçéá ìá òì ppp(8) (*user-ppp*) èÛ ðññðá íá ääßóá èÛóέ ðñññññέì ìá òì ðññáέÛóò:

```
% 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...)
```