


```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεεᾶ οᾶβ÷ἰοο δñἰοᾶόβαο οἰῶ δῶñΠία.

ΌγίαΒυός: Άόου όι έαβιαί έαυηάβ υόε Ύ÷ άόά άαέάόάόόΠόάέ όγι Ύέαιός 5.X όιό FreeBSD Π ιέα όεί όηύόόάό. Άί ÷ήόόέίόίέαβόά όγι Ύέαιός 4.X, όύόά έά όηΎόάέ ίά άίάηάίόίέΠόάόά όγι άόέέϊΆ *IPFW2* έάέ ίά άέάάΎόάόά ός όάέβάά άίΠεάέό ipfw(8) έέά όηέόόόύόόηάό όέόηίόίηβάό ό÷ άόέέΎ ίά όγι άόέέϊΆ *IPFW2*. ΠηίόΎίόά έάέάβόάηά όι όίΠιά *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFWALL_VERBOSE
```

ÓôÝéíáé ôá ìçíýíáôá äéá ôá éáoÜëëçéá ðáéÝôá óôi log ôiõ óõóôÞíáôîð.

```
options IPFWIREWALL_VERBOSE_LIMIT=500
```

Ἄϋααε εὐϋιεῖ νηεῖ ὁδεὸ νινῤο θῖο εὐϋιεά αααῆαοP εα εαὸαανῤοαὸαε. ὃοε ἰθῖηαβὸα ἰά εαὸαανῤοαὸα ὁά ἰςῖῖαὸα αῖυ ὅῖ ὁαβ÷ῖθ θῖηῖοαὸαβὸ ÷ῖηβὸ ὅῖ εβῖαῖῖ ἰά ααἰβὸῖῖ ὁά αῖ÷ῖα εαὸααῆαοP ὁῖο ὁῶῶPἰαὸαυ ὁά ἰα αα÷ῖαβὸα εὐϋιεά αῖβεαὸς. Ὅῖ νηεῖ 500 ἰςῖῖῤοῖ αβῖάε ἰεά αῆεαῖῤ εῖαεεP ὀειP, αεεῖῤ ἰθῖηαβὸα ἰά θῖῖοαῖῖῤοαὸα αῶῶP ὀςῖ ὀειP ἰῖῖῖῖα ἰά ὀεὸ αῖαεῶPῖαεὸ ὅῖο αεεῖῖ ὁά αεεῖῖῖῖ.

```
options IPDIVER
```

Āīāñāīđīēāß ôā *divert* sockets, đĩō èā āīyĩā āñāūôāñā ôē ēŬĩĩĩ.

[illegible]

3 ÁëëáãỲò óôi /etc/rc.conf ãéá íá öĩñôþíáôáé ôĩ ôâß÷ìò
ðñĩóôáóßáò

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 áīçīāñþróāōā 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 έάέάίέŨó άóü άóóŸó όέó áñáiŸó, ñßíόά ίέα ίάόέŨ όόί /etc/default/rc.conf έάέ έέάáŨóόά όçí man óάëßää rc.conf(5)

4 ΆíññìðìέΠóòά όçí ΑίóύìáòùìΎίç ìáòÛññάόç Äέáðēýíóáùì óìò PPP

Άέά íá äðέòñÝðáòά óá Ûέέá ìç÷áíΠíáóá όìò äέέóýìò óáò íá óóíáÝìíóáέ ìá όìì Ýìù έùóìì ìΎóù όìò FreeBSD, ÷ñçóέììðìέΠíóáò όì ùò “ðýέç”, έá ðñÝðáέ íá áíñññìðìέΠóòάά όçí ΑίóύìáòùìΎίç ìáòÛññάόç äέáðēýíóáùì όìò PPP (NAT). Άέά íá áβίáέ áòòù, ðñìóέΎóóá όóì áñ÷áβì /etc/rc.conf όέò ðáñáέÛòù áñáñìΎò:

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

Όόç èΎόç όìò ðñìòβέ_όçò_όγíááόçò ðñÝðáέ íá áÛέáòά όì ùíñá όçò óγíááóΠò óáò, ùòòù όì Ύ÷áòά áðìέçέáýóáέ όóì áñ÷áβì /etc/ppp/ppp.conf.

5 Ìέ έáíüíáò όìò firewall

Όì ìüñì όìò áðñìΎíáέ όΠñá áβίáέ íá ìñβóìòìá όìòò έáíüíáò όìò firewall. Ìέ έáíüíáò όìòò ìðìβìòò ðáñέáñÛóìòìá ááΠ áβίáέ áñέáòÛ έáέìβ áέá όìòò ðáñέóóùòáñìòò ÷ñΠóóáò ìá dialup óγíááόç, áέέÛ ìýóá όðì÷ñáùóέέìβ áβίáέ, ìýóá áβίáέ áóíáòùì íá óáέñέÛέìòì ìá όέò áíÛáέáò ùέùì óùì ÷ñçóóΠí dialup. Ìðìñìýì, ùìò, íá ÷ñçóέìáýóìòì ùò Ύíá έáέù ðáñÛááέáìá ñòέìβóáùì όìò IPFW έáέ áβίáέ ó÷áòέέÛ áýέìì íá όìòò ðñìóáñìüóáòά óóέò äέέΎò óáò áíÛáέáò.

Áò áñ÷βóìòìá ùìò ìá όέò ááóέέΎò áñ÷Ύò áíüò έέáέóóìý óáβ÷ìòò ðñìóóáóáò. Íá έέáέóóù óáβ÷ìò ðñìóóáóáò áðááññáýáέ έáò’ áñ÷Πí έÛέá óγíááόç. Ì áέá÷áέñέóóΠò ìðìñáβ ýóóáñá íá ðñìóέΎóáέ έáíüíáò áέá íá äðέòñÝðáέ ìüñì óóáέáñέñέìΎíáò óóíáΎóáέò íá ðáñìÛíá áðù όì óáβ÷ìò ðñìóóáóáò. Ç ðέì óðìçέέóìΎίç óáέñÛ óùì έáíüíüí óá Ύíá έέáέóóù óáβ÷ìò áβίáέ: ðñΠóá ìέ έáíüíáò όìò äðέòñÝðìòì ìáñέέΎò óóíáΎóáέò, έáέ óÝέìò ìέ έáíüíáò όìò áðááññáýìòì ìðìέááΠðìòά Ûέέç óγíááόç. Ç έìáέέΠ ðβóù áðù áòòù áβίáέ ùóέ ðñΠóá áÛááòά όìòò έáíüíáò όìò äðέòñÝðìòì ðñÛáíáóá íá ðáñÛóìòì έáέ ýóóáñá ùέá óá Ûέέá áðááññáýìíóáέ áòòùìáóá.

ΌóέÛìòά, έìέðüì, Ύíá έáòÛέìáì óóìì ìðìβì έá áðìέçέáýìíóáέ ìέ έáíüíáò όìò óáβ÷ìòò ðñìóóáóáò. Óá áòòù όì Ûñέñì ÷ñçóέììðìέìýìá ùò ðáñÛááέáìá όìì έáòÛέìáì /etc/firewall. ΆέέÛìòά έáòÛέìáì ìΎóá óá áòòùì έáέ äçìέìòñáΠóóá όì áñ÷áβì fwrules όìò όì ùíñÛ όìò áβ÷áìá áñÛáέ όóì rc.conf. ÓçìáέΠóóá ðùò ìðìñáβóá íá áέέÛìáòά όì ùíñá όìò áñ÷áβìò áòòìý óá ùóέ èΎέáòά. Áòòùò ì ìäçáùò áβίáέ áòòù όì ùíñá óáí ðáñÛááέáìá έáέ ìüñì.

Áò äìýìá όΠñá Ύíá ðáñÛááέáìá óáβ÷ìòò ðñìóóáóáò ìá áñέáòÛ áðáíçäçìáóέέÛ 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
```

Όπná Ý÷áoá Ýía ðēēçñüíÝíí óåβ÷ìð ðñüóóáóβáo, òì ìðìβì óðíaÝóáéð óðéð èýñåð 22 éáé 80 éáé éáoáñÜöåé üēåð óéð Üēēåð óðíaÝóáéð óôi åñ÷åβì éáoáñåöðð òìð óóóðßíåðìð. ÐēÝíí åβóðå Ýðìēñē áéå åðáíåēßçóc. Ôì óåβ÷ìð ðñüóóáóβáo éå áíåñåðìçēçåß åðöüííåð éåé éå öìñðóåé òìð éåíüíåð ðìð ðñìóēÝóáðå. Áí åå åβíåé åðöü Þ Ý÷áoå ððìéååßðìåð ðñíåßßåðå, Þ áí Ý÷áoå èÜðìéåð ðñìÜóáéð áéå íå áéññēñēåß åðöü òì Üñēñì, åðéçìñüíßóåð íåßß ìð ìå email.

6 Åñüòßåéò

1. ÅēÝðü ìçíýíåð üðüð limit 500 reached on entry 2800 éåé ìåðÜ åðü òì óýóçìÜ ìð óðåíåðÜåé íå éáoáñÜöåé óå ðåēÝóå ðìå åìðñåñíåðåé åðü òì óåβ÷ìð ðñüóóáóβáo. Åìçåýåé åéñüå òì firewall ìð;

Åðöü åðēÜ óçíåßíåé ðüð Ý÷åé ðñçóēñìðçēçåß òì ìÝåóòì üñēñ éáoáñåöðð (logging) áéå åðöü òì éåíüíå. Ì éåíüíåð ì ßåìð åíåçìçēðåß íå åìçåýåé, åēÜ ååñ éå óóÝçíåé ðéå ìçíýíåð óôi åñ÷åβì éáoáñåöðð òìð óóóðßíåðìð ìÝ÷ñé íå ìçåñíåðåð ðÜçē òìð ìåñççÝð. Ìðñåßðå íå ìçåñíåðåð òìð ìåñççÝð ìå ççí åñìçÞ

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðñáóáðá òñ ùñέì éάóáññáöðò óóέò ñòèìβóάέò òñ ððñá íá óáò ìá òçí áðέέìáÐ IPFWALL_VERBOSE_LIMIT ùðòð ðáñέáñÛðáì ðáñáðÛñ. Ìðññáβóá íá áέέÛíáðá áðóó òñ ùñέì (÷ ùñβò íá ìáðááèòóóβóáðá ðÛέέ òñ ððñá íá óáò éάέ íá èÛíáðá reboot) ÷ ñçóέììðìέðíðáð òçí sysctl(8) óέìÐ net.inet.ip.fw.verbose_limit.

2. ÈÛðìέì èÛèò ðñÝðáέ íá Ýáέíá. Áέèìýçóá óέò áíòìÝð éáðÛ ãñÛíá éάέ òþñá èèáέäþèçéá áðÝñ.

Áðóóò ì ìäçáòð òðìèÝðáέ ùðέ ÷ ñçóέììðìέáβóá òñ *userland-ppp*, áέ áðóó èέ ìέ éáfííáð ðñò áβñíóáέ ÷ ñçóέììðìέíý òñ tun0 interface, ðñò áíóέóðìέ÷ áβ óðçí ðñþòç óýíááóç ðñò óðέÛ÷ íáðáέ ìá òñ ppp(8) (áέέέðò áñóóó èάέ ùð *user-ppp*). Ç áðñíáíç óýíááóç éá ÷ ñçóέììðìέíýóá òñ tun1, ìáðÛ òñ tun2 éάέ ðÛáέ èÝáñíðáð.

Èá ðñÝðáέ áðβóçò íá èòìÛóðá ùðέ òñ pppd(8) ÷ ñçóέììðìέáβ òñ interface ppp0, ìðóðá áí ìáέέíáóáðá òç óýíááóÐ óáò ìá òñ pppd(8) éá ðñÝðáέ íá áíóέéáóáóðáóðá òñ tun0 ìá ppp0. ÐáñáέÛóó èá ááβñíðá Ýíá áýέèì ðñóðñ íá áέέÛíáðá òñòð éáfííáð òñò firewall éáðÛέçéá. Ìέ áñ÷έέìβ éáfííáð òþæííóáέ 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
```

Άέά íá éáðáέÛááðá áí ÷ ñçóέììðìέáβóá òñ ppp(8) Ð òñ pppd(8) ìðññáβóá íá áñáðÛóáðá òçí Ýññáì òçò ifconfig(8) áóñý áñáñáñðìέçéáβ ç óýíááóÐ óáò. Ð.÷., áέá ìέá óýíááóç ðñò áñáñáñðìέçéçéá áðó òñ pppd(8) éá ááβðá èÛóέ óáf áðóó (ááβ÷ñíðáέ ìññ ìέ ò÷áðέéÝð ãñáñÝð):

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

Άðó òçí Ûέέç, áέá ìέá óýíááóç ðñò áñáñáñðìέçéçéá ìá òñ ppp(8) (*user-ppp*) èÛ ðñáðá íá ááβðá èÛóέ ðáñññìέì ìá òñ 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...)
```