

# Όγιάαός ΙΎού Όçäåöþñĩ òéé Ôåß÷ìò Ðñĩóôáóßàò óôĩ FreeBSD

Marc Silver

marcs@draenor.org

\$FreeBSD: doc/el\_GR.ISO8859-7/articles/dialup-firewall/article.sgml,v 1.20  
2008/12/08 03:10:51 keramida Exp \$

Ôĩ FreeBSD áβιάέ Υία éáôĩ÷õñùìΥĩ ãìðñééÛ óγìãñē òĩò FreeBSD Foundation.  
ÐñēēΥò áðù óéò ēΥìáéò ð õñÛóáéò ìé ìðĩßàò ÷ ñçóéììðñēìγìóáé áðù òĩòò éáóáóéãáóóðΥò ð òĩòò  
ðùεçòΥò òĩòò áéá íá áéáéñññĩòĩ óá ðñĩùìíóá òĩòò éãùññĩγìóáé ãìðñééÛ óγìãñē. ¼ðìò áóðΥò  
ãìðáíβæìíóáé óá áóðù òĩ éãßìãñ éáé áéá ùóáò áðù áóðΥò ãìùññæáé ç ììÛáá ÁíÛðððçò òĩò FreeBSD ùóé  
åβιάé ðééáìíí íá áβιάé ãìðñééÛ óγìãñē, éá åãßòå Υία áðù óá óγìãñē: “TM” ð “®”.

Áóðù òĩ Ûñēñ ðãñéãñÛóáé ðùò ìðñãßòå íá ñðèìßóãòå Υία ôåß÷ìò ðñĩóôáóßàò (firewall) ÷ ñçóéììðñēìγìóáò  
ìéá PPP óγìãñēç ìΎóù òçäåöþñĩò óôĩ FreeBSD ìå òĩ IPFW. Ðéì óðæãñéñçΥία, ðãñéãñÛóáé òç ñγέìέçç áìùð  
ôåß÷ìò ðñĩóôáóßàò óá ìéá óγìãñēç ìΎóù òçäåöþñĩò ðìò Υ÷áé äóíãíέçç IP áéãýðçíçç. Áóðù òĩ éãßìãñ äãí  
áç÷ìåãßóáé ìå òĩ ðùò éå ñðèìßóãòå òçí äñ÷έçç óáð óγìãñēç ìΎóù PPP. Áéá ðãñéóóóðãñåð ðεçññìññßàò  
ó÷ãðééÛ ìå ðéð ñðèìßóáéð ìéáð óγìãñēç ìΎóù PPP åãßòå òç óåßßåä ãñðéåáð ppp(8).

## 1 Ðñüēñĩò

Áóðù òĩ éãßìãñ ðãñéãñÛóáé òçí áéãáééáóßå ðìò ÷ ñåéÛæåóáé áéá íá ñðèìßóãòå Υία ôåß÷ìò ðñĩóôáóßàò óôĩ  
FreeBSD ùóáí ç IP áéãýðçíçç äβíáóáé äóíãíέçç áðù òĩ ISP óáð. Ðãññüē ðìò Υ÷ù ðñĩóðæçðóáé íá èÛù áóðù òĩ  
éãßìãñ ùóí òĩ äóíãíüñ ðéì ðεðñåð éáé óùóðù, åβóðå äððñüóåãðéé íá óðåßéðå ðéð äéññèðóáéð, óá ó÷üééá ð ðéð  
ðñìòÛóáéð óáð òçç áéãýðçíçç òĩò óðããñåðΥία: <marcs@draenor.org>.

## 2 ÐãñÛìåðññé òĩò ððññíá

Áéá íá ìðñΥóáðå íá ÷ ñçóéììðñēìγìóáð òĩ IPFW, ðñΥðåé íá áíóóìåððóãòå òçí ó÷ãðééç ððññññéçç óôñ ððññíá óáð.  
Áéá ðãñéóóóðãñåð ðεçññìññßàò ó÷ãðééÛ ìå òç ìåðåãðððéçç òìò ððññíá, åãßòå òĩ òìñíá ñðèìßóãòå òìò ððññíá óôñ  
Åã÷áéñßåñ (http://www.FreeBSD.org/doc/el\_GR.ISO8859-7/books/handbook/kernelconfig.html). Èå ðñΥðåé íá  
ðññéçΥóáðå ðéð ðãñééÛ ððéçñññç òéð ñðèìßóáéð òìò ððññíá óáð áéá íá áíãññðñéçðóáð òçí ððññññéçç áéá òĩ  
IPFW:

```
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*. ΌηιόΎίόά 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 ÁëéãÿÒ óôï /etc/rc.conf äéá íá öïñôþíáôáé ôï ôâß÷ìò  
ðñïóôáóßàò

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"
```

Ääá äðäöóüöñâð ðëçñïòíñBåð ö-äöéÜ íà ðç óçíáöBåð éäéäíéÜð áðu áðöÝð öéð äñànÝð, ñBíôä íéä íäöéÜ öðí /etc/defaults/rc.conf éäé äéääÜöðä öçí man öäèBää rc.conf(5)

## 4 ΆíññìðìéΠóóå ôçí ΆíóύìáòùìΎìç ìåðÛññåç Äéåðëýíóåùì óìò 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 άíóύìáòùìΎìç ìåðÛññåç äéåðëýíóåùì òìò PPP (NAT). Άέå íå åβíåé åðòù, ðñìéÝóåå óòì åñ÷åíìåå /etc/rc.conf òéð ðåñåÛòù åñåñìÝð:

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

Όçç èΎçç òìò ðñìððë\_ðçð\_όγιάååçð ðñÝðåé íå åÛëååå òì ùñåå ççð óýìååðð òåð, ùðòù òì Ύ÷ååå äðìçëåýóåé óòì åñ÷åíìåå /etc/ppp/ppp.conf.

## 5 Ìé éåíüìåò òìò firewall

Όì ìññ ðìò äðñÝíåé ðññå åβíåé íå ìñβòìåå òìò éåññåå òìò firewall. Ìé éåññåå òìò ìðìβìòð ðåñåñÛòììåå ååð åβíåé åñëåðÛ éåññ åéå òìòð ðåñåóóùðåñìòð ÷ñΠóóåå ìå ðìåð óýìååç, åëëÛ ìýåå òðì÷ñåðéì åβíåé, ìýåå åβíåé åðíååùì íå óåññÛåñì ìå òéð åñÛååð ùëù òùì ÷ñçóðì ðìåð. Ìðññýì, ùìð, íå ÷ñçóëìåýóòì ùð Ύíå éåëù ðåñÛåéåñì ðòëìβååùì òìò IPFW éåé åβíåé ó÷åðéëÛ åýëìì íå òìòð ðñìóåñìùóååå óééð åéëÝð óåå åñÛååð.

Áð åñ÷åíìåå ùìð ìå òéð ååóéëÝð åñ÷Ýð åññð èëåóóòý òåβ÷ìòð ðñìóóååå. ìå èëåóóòù òåβ÷ìòð ðñìóóåååå åðåññåýåé ååð’ åñ÷Πì èÛëå óýìååç. Ì åéå÷åñéóóðð ìðññåå ýóóåñå íå ðñìéÝóåé éåññåå åéå íå äðéòñÝðåé ìññ óåååññåñìÝíåå óðíåÝóåé íå ðåññÛíå åðù òì òåβ÷ìòð ðñìóóååå. Ç ðëì óðìçééçìΎìç óåññÛ òùì éåñññì óå Ύíå èëåóóòù òåβ÷ìòð åβíåé: ðñðåé ìé éåññåå ðìò äðéòñÝðìì ìåñéëÝð óðíåÝóåé, éåé òÝëì ìé éåññåå ðìò äðåññåýìì ìðìåååððìåå Ûëçç óýìååç. Ç ëñåçëΠ ðβòù åðù åðòù åβíåé ùéð ðñðåé åÛåååå òìòð éåññåå ðìò äðéòñÝðìì ðñÛåñåå íå ðåñÛòìì éåé ýóóåñå ùëå óå Ûëëå äðåññåýìíóåé åðòùìåå.

ΌéëÛìåå, ëëðùì, Ύíå éåðÛëñì óòì ìðìβì éå äðìçëåýìíóåé ìé éåññåå òìò òåβ÷ìòð ðñìóóååå. Όå åðòù òì Ûñëñì ÷ñçóëìðìéýìå ùð ðåñÛåéåñì òìì éåðÛëñì /etc/firewall. ΆéëÛìåå éåðÛëñì ìΎóå óå åðòùì éåé åçìéìðñåΠóóåå òì åñ÷åíìåå ðìò òì ùññÛ òìò åβ÷åñì åñÛåé óòì rc.conf. ΌçñåéΠóóåå ðùð ìðññååå íå åéëÛìåå òì ùñåå òìò åñ÷åíìåå åðòý óå ùéð èΎëååå. Áðòùð ì ìåçåð åβíåé åðòù òì ùñåå óåñ ðåñÛåéåñì éåé ìññ.

Áð åñýìå ðññå Ύíå ðåñÛåéåñì òåβ÷ìòð ðñìóóåååå 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÷áoά Ύía ðèèçñüìÝíí óαβ÷ιò ðñüóóáóβáo, òì ìðìβì óðíaÝóáέò óóέò èýñáo 22 έάέ 80 έάέ έáoáñŮóάέ üέáo óέò Üέέáo óðíaÝóáέò óôi áñ÷άβì έáoáññáoðò òìò óóóðβíaóìò. ÐèÝíí άβóóά Ύòìèíé άέά άðáíάέέβίçóç. Όì óαβ÷ιò ðñüóóáóβáo έά áíáñáñðìέçέάβ άóòüíáóά έάέ έά òìòðóάέ òìòò έáíüíáo ðìò ðñìóèÝóάóά. Áí άά άβíάέ άóòü Þ Ý÷áoά ððìέάáððìóά ðñíάèβíaóά, Þ áí Ý÷áoά èŮðìέáo ðñìóŮóáέò άέά íá áéíñèùέάβ άóòü òì Ůñèñí, άðέέìéíüíβóóά íάέβ ììò íá email.

## 6 Άñùòβóάέò

1. ΆέÝðü ìçíýíáóά üðüò “limit 500 reached on entry 2800” έάέ íáoŮ άðü άóòü òì óýóòçìŮ ììò óðáíáoŮάέ íá έáoáññŮóάέ óά ðάέÝóά ðìò άìðñáβæííóάέ άðü òì óαβ÷ιò ðñüóóáóβáo. Άìòέáýάέ áéüíá òì firewall ììò;

Άóòü άðèŮ óçíáβíάέ ðüò Ý÷άέ ÷ñçóèíðìέçέάβ òì ìÝάέóòì üñéí έáoáññáoðò (logging) άέά άóòü òì έáíüíá. Ì έáíüíáo ì βάέìò áíáèìèìòέάβ íá äìòέáýάέ, áέèŮ ááí έά óóÝèíάέ ðéá ìçíýíáóά óôi áñ÷άβì έáoáññáoðò òìò óóóðβíaóìò ìÝ÷ñέ íá ìçáíñβóóά ðŮέέ òìòò ìáoñçòÝò. Ìðñíáβóά íá ìçáíñβóóά òìòò ìáoñçòÝò ìά òçí áíòìèÞ

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáßóá íá áõìßóáóá òì ùñéì éáóáññáößò óóéò ñòèìßóáέò òìò ðòñßíá óáò ìá òçì áðéëíäß IPFWALL\_VERBOSE\_LIMIT ùðòò ðññéññÛðáì ðññáðÛñ. ìðññáßóá íá áέέÛíáóá áóòò òì ùñéì (÷ ùñßò íá ìáóáæèòóóßóáò ðÛέέ òì ðòñßíá óáò éάέ íá èÛíáóá reboot) ÷ ñçóéììðéííóáò òçì sysctl(8) óéìß net.inet.ip.fw.verbose\_limit.

2. ÈÛðéì èÛèò ðñÝðáé íá Ýáéíá. Áéëéýçóá óéò áíóñéÝò éáóÛ ãñÛíá éάέ òþñá èéáéäþççéá áðÝñ.

Áóòòò ì ìäçäùò òðñéÝðáé ùóé ÷ ñçóéììðéíáßóá òì *userland-ppp*, áé áóòò èé ìé éáfííáð ðìò äßñíóáé ÷ ñçóéììðéíéýì òì tun0 interface, ðìò áíóéóóé÷÷ äß óóçì ðñþòç óýíááóç ðìò óóéÛ÷ íáóáé ìá òì ppp(8) (áéçéðò áñóòò éάέ ùò *user-ppp*). Ç áðñíáíç óýíááóç éá ÷ ñçóéììðéíéýóá òì tun1, ìáóÛ òì tun2 éάέ ðÛáé èÝáñíóáò.

Èá ðñÝðáé áðßóçò íá èòìÛóóá ùóé òì pppd(8) ÷ ñçóéììðéíáß òì interface ppp0, ìðòòá áí ìáééíßóáóá òç óýíááóß óáò ìá òì pppd(8) éá ðñÝðáé íá áíóééáóóóßóáò òì tun0 ìá ppp0. ÐññáéÛòò éá ääßñíóá Ýíá áýçéì ðññðì íá áέέÛíáóá òìòò éáfííáð òìò firewall éáðÛέççéá. ìé áñ÷ééìß éáfííáð òþæííóáé óá Ýíá áñ÷äß 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 ÷ ñçóéììðéíáßóá òì ppp(8) ð òì pppd(8) ìðññáßóá íá áñáóÛóáóá òçì Ýññäì òçò ifconfig(8) áóñý áñññäñðéççéä ç óýíááóß óáò. Ð.÷., áέá ìéá óýíááóç ðìò áñññäñðéççéä áðò òì pppd(8) éá ääßóá èÛóé óáí áóòò (ääß÷ñíóáé ìñì ìé ò÷äóééÝò ãñññÝò):

```
% 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 áñññäñðéççéä ìá òì ppp(8) (*user-ppp*) èÛ ðññðá íá ääßóá 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...)
```