

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 ïé ïðĩßàò ÷ 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 ÁíÛððçìçò 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 ðñĩóóáóßàò (firewall) ÷ ñçóéììðñēìγìóáò
ìéá PPP óγìãñēç ìΎóù òçäåöþñĩò óôĩ FreeBSD ìå òĩ IPFW. Ðéì óðæãñēçìΥία, ðãñéãñÛóáé çç ñγέìέçç áìùð
ôåß÷ìò ðñĩóóáóßàò óá ìéá óγìãñēç ìΎóù òçäåöþñĩò ðìò Υ÷áé äóíãíέçç IP áéãýðçìçç. Áóðù òĩ éãßìãñ äãí
áç÷ìåãßóáé ìå òĩ ðùò éá ñðèìßóãòå ççí áñ÷έçç óáð óγìãñēç ìΎóù PPP. Áéá ðãñéóóóðãñåð ðεçññìññßàò
ó÷ãðééÛ ìå ðéò ñðèìßóáéò ìéáð óγìãñēç ìΎóù PPP åãßòå çç óåßãåå ãñðéåáð ppp(8).

1 Ðññēñĩìò

Áóðù òĩ éãßìãñ ðãñéãñÛóáé ççí áéãåééáóßá ðìò ÷ ñåéÛæåóáé áéá íá ñðèìßóãòå Υία ôåß÷ìò ðñĩóóáóßàò óôĩ
FreeBSD ùóáí ç IP áéãýðçìçç äβíáóáé äóíãíέçç áðù òĩ ISP óáð. Ðãññēç ðìò Υ÷ù ðñĩóðæçðóáé íá èÛù áóðù òĩ
éãßìãñ ùóí òĩ äóíãíέçç ðéì ðεðñåð éáé óùóðù, åβóðå äððñùóåãðéé íá óðåßéåðå ðéò äéññèðóáéð, óá ó÷ùééá ð ðéò
ðñìòÛóáéð óáð óçç áéãýðçìçç òĩò óðããñåðΥία: <marcs@draenor.org>.

2 ÐãñÛìåðññé òĩò ððññíá

Áéá íá ìðñΥóáðå íá ÷ ñçóéììðñēìγìóáò òĩ IPFW, ðñΥðåé íá áìóùìåððóãòå ççí ó÷ãðééç ððññññéçç óôñ ððññíá óáð.
Áéá ðãñéóóóðãñåð ðεçññìññßàò ó÷ãðééÛ ìå çç ìåóåãèððééç òìò ððññíá, åãßòå òĩ òìñíá ñðèìßóãòå òìò ððññíá óôñ
Åã÷áéññäéç (http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html). Èá ðñΥðåé íá
ðññéçΥóáðå ðéò ðãñééÛðù äðéçñΥð óðéò ñðèìßóáéð òìò ððññíá óáð áéá íá áñãñãñðñéçç ðóãòå ççí ððññññéçç áéá òĩ
IPFW:

```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεεᾶ οᾶβ÷ἰοο δñιόοᾶόβαο οἰῶ δῶñΠία.

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

```
options IPFWALL VERBOSE
```

ÓôÝéíáé ôá ìçíýíáôá ãéá ôá éáôÜëëçéá ðáéÝôá óôî log ôîõ óõóôÞíáôîð.

```
options IPFWIREWALL VERBOSE LIMIT=500
```

[illegible]

```
options IPDIVER
```

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

[illegible]

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

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

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

Ääá äðäéöóüöñâño ðëçñïöïñBão ó-äöéêÜ íà öç öçíáöBáo éäéäîéÜò áðu áðöÝò öéò äñànìÝò, ñBíôä íéä íäöéÜ ööí /etc/defaults/rc.conf éäé äéääÜöðä öçí man öäèßää rc.conf(5)

4 ΆíññìðìéΠóóå ôçí ΑίóύìáòùìΎìç ìåðÛññåç Äéåðëýíóåùì òìò PPP

Άέά íá äðéòñÝðååå óå Ûëëá ìç÷áíìáåå òìò äééðýìò óåó íá óðíáÝìíóåé ìå òìì Ýìù èùòì ìΎóù òìò FreeBSD, ÷ñçóëìðìéðìåðìåð òì ùð “ðýëç”, åå ðñÝðåé íá áíñññìðìéΠóóåå ôçí ΑίóύìáòùìΎìç ìåðÛññåç äéåðëýíóåùì òìò PPP (NAT). Άέά íá äáíåé áðòù, ðñìéÝóåå óòì áñ÷áñì /etc/rc.conf ðéð ðåñåÛòù äñåñìÝð:

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

Όçç èΎçç òìò ðñìððë_ðçð_όγιάαός ðñÝðåé íá åÛëååå òì ùñå ççð óýìååðð ðåð, ùðò òì Ύ÷åå äðìçëåýóåé óòì áñ÷áñì /etc/ppp/ppp.conf.

5 Ìé éåíüìåò òìò firewall

Όì ìññ ðìò äðñÝíåç ðññå ááíåé íá ìñóìñìå ðìò éåññåð òìò firewall. Ìé éåññåð ðìò ìðìðìò ðåñåñÛòìñìå äåð ááíåé áñëåðÛ éåññ åéå ðìò ðåñéóóùðññìò ÷ñΠóóåå ìå ðìåð óýìååç, äéëÛ ìýåå ððì÷ñåðéñ ááíåé, ìýåå ááíåé äñíåðùì íá óåññÛåñì ìå ðéð áñÛååð ùëù ðùì ÷ñçóðñì ðìåð. Ìðññìý, ùñð, íá ÷ñçóëìåýóìñì ùð Ύíå éåëù ðåñÛåéñì ððëìðåùì òìò IPFW éåé ááíåé ó÷åðéëÛ åýëñì íá ðìò ðñìóåñìóååå óéð äéëÝð ðåð áñÛååð.

Áð áñ÷óìñìå ùñð ìå ðéð ååóéëÝð áñ÷Ýð áñùð èëåóóìý ðåβ÷ìò ðñìóóååå. ìå èëåóóù ðåβ÷ìò ðñìóóååå äåñññåýå éåð’ áñ÷ðì èÛëå óýìååç. Ì åéå÷åñéóðð ìðññåç ýóóåñå íá ðñìéÝóåé éåññåð åéå íá äðéòñÝðåé ìññ óåååñññìÝíåð óðíáÝóåð íá ðåññÛíå äðù òì ðåβ÷ìò ðñìóóååå. Ç ðéì óðìçéóìΎìç óåññÛ ðùì éåñññì óå Ύíå èëåóóù ðåβ÷ìò ááíåé: ðñðå ìé éåññåð ðìò äðéòñÝðìñ ìåñéÝð óðíáÝóåð, éåé ðÝëì ìé éåññåð ðìò äðåññññìñì ìðìååððìñå Ûëçç óýìååç. Ç ëñåçð ðβòù äðù áðòù ááíåé ùé ðñðå åÛååå ðìò éåññåð ðìò äðéòñÝðìñ ðñÛåñåå íá ðåñÛòìñ éåé ýóóåñå ùëå óå Ûëëå äðåññññìñåé áðòùñåå.

ΌðéÛìå, ëñðùì, Ύíå éåðÛëñì óòì ìðìñ åå äðìçëåýìñåé ìé éåññåð ðìò ðåβ÷ìò ðñìóóååå. Όå áðòù òì Ûñëñì ÷ñçóëìðìéýñì ùð ðåñÛåéñì òì éåðÛëñì /etc/firewall. ΆéëÛìå éåðÛëñì ìΎóå óå áðòù éåé ðçìéìñåΠóóåå òì áñ÷áñì fwrules ðìò òì ùñÛ ðìò åβ÷åñå ðñÛåç óòì rc.conf. Όçñåçðåå ðùð ìðñåβåå íá äéëÛååå òì ùñå òì áñ÷áñì áðòìý óå ùé èΎëåå. Áðòù ì ìåçåð ááíåé áðòù òì ùñå óå ðåñÛåéñì éåé ìññ.

Áð åññå ðññå Ύíå ðåñÛåéñì ðåβ÷ìò ðñìóóååå ìå áñëåðÛ äðñçåçñåéëÛ ó÷ëëå.

```
# 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
```

[illegible]

6 ĀñûôṖóǎéò

1. ἈέΨδου ιερίγλαόα υἱδὸν “limit 500 reached on entry 2800” ἐὰς λαόϚ ἀδου αὐοῦ οἱ γύοόϙι ὡρ ὁάηαόϚ ἄε ἰά
ἐαόαανᾤϚ ὁα θαέΨόα δῖος ἀιδραβᾤρῖσῶας ἀδου οἱ ὁάβ÷ῖδ ὀνῖοόαόβασ. Ἀῖρεᾤᾤας ἀεὺηα οἱ firewall ἡῖρ;

Ἀδοῦ ἀδῆῦ ὁγιὰβῖαῖ δὺδ ὕ ÷ ἁῖ ÷ ἡγοῖνῖθῖεῖαῖβ ὁῖ ἰὺἁῖοῖ ὑνῖ ἑάοἁἡἡἁῖβ (logging) ἁῖἁ ἁδῶ ὁῖ ἑἁῖῖἁ. Ἰ ἑἁῖῖἁ ἰ
 βᾱῖῖ ἁῖἁῖῖῖῖῖἁ ἰἁ ἁῖῖἁῖἁ, ἁῖῖῖ ἁῖ ἑἁ ὁδὺῖἁῖ ῥῖ ἰγιῖἁῖ ὁῖ ἁῖ ÷ ἁῖ ἑἁἁἡἡἁῖβ ὁῖ ὁῖὁῖἁῖἁῖ ἰὺ ÷ ἡῖ ἰἁ
 ἰῖἁἁἁῖὁἁῖ ῥῖῖ ὁῖὁ ἰἁἡἡῖῖ. Ἰῖἡἡὁἁ ἰἁ ἰῖἁἁἁῖὁἁ ὁῖὁ ἰἁἡἡῖῖ ἰἁ ὁῖ ἁῖῖῖ

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðìþóáðá òì ùñέì éάóáññáðòðò óóέò ñðèìβóáέò òìò ððñþíá óáo ìá όçì áðέέìāþ IPFWALL_VERBOSE_LIMIT ùðòð ðññέññÛðáì ðññáððÛñ. ìðññáβóá íá áέέÛíáðá áðóò òì ùñέì (÷ ùñβò íá ìáðáάέùòðβóáðá ðÛέέ òì ððñþíá óáo éάέ íá éÛíáðá reboot) ÷ ñçóέììðìέþíðáo όçì sysctl(8) όέìþ net.inet.ip.fw.verbose_limit.

2. ÊÛðìέì éÛέìò ðñÝðáέ íá Ýáέíá. Áέέìýçέóá óέò áíòìéÝð éáoÛ ãñÛìá éάέ όþñá éέάέäþέçéá áðÝñ.

Άðóòò ì ìäçäùð òðìéÝðáέ ùðέ ÷ ñçóέììðìέáβóá òì *userland-ppp*, áέ áðóò éέ ìé éáfííáð ðìò áβñíðáέ ÷ ñçóέììðìέìýì òì tun0 interface, ðìò áíðέóðìέ÷ áβ óόçì ðñþόç óýíááόç ðìò óðέÛ÷ íáðáέ ìá òì ppp(8) (áέέέþð áñóðò éάέ ùð *user-ppp*). Ç áðùìáìç óýíááόç éá ÷ ñçóέììðìέìýóá òì tun1, ìáðÛ òì tun2 éάέ ðÛáέ éÝáñíðáo.

Éá ðñÝðáέ áðβόçò íá èòìÛóðá ùðέ òì pppd(8) ÷ ñçóέììðìέáβ òì interface ppp0, ìðòðá áí ìáέέìþóáðá όç óýíááόþ óáo ìá òì pppd(8) éá ðñÝðáέ íá áíðέéάóáóðþóáðá òì tun0 ìá ppp0. ÐññáέÛòù éá ááβñìòìá Ýíá áýέìέì ðñùðì íá áέέÛíáðá òìòò éáfííáð òìò firewall éáoðÛέέçéá. ìé áñ÷έέìβ éáfííáð όþæìíðáέ 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) þ òì pppd(8) ìðññáβóá íá áíáðÛóáðá όçì Ýññäì όçò ifconfig(8) áóìý áíáññäìðìέçéáβ ç óýíááόþ óáo. Ð.÷., áέá ìéá óýíááόç ðìò áíáññäìðìέþέçéá áðù òì pppd(8) éá ááβðá éÛóέ óáf áðóò (ááβ÷ñíðáέ ìùì ìé ó÷áðέέÝð ãññäìÝð):

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

Άðù όçì Ûέέç, áέá ìéá óýíááόç ðìò áíáññäìðìέþέçéá ìá òì ppp(8) (*user-ppp*) èÛ ðññðá íá ááβðá éÛóέ ðññññέì ìá òì ðññáέÛòù:

```
% 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...)
```