

Όγιάαός ΙΎού Όçäåöþñĩ òéé Ôåß÷ìò Ðññíóôáóßàò 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÷õññìΥĩ ãìðñééÛ óγìãñē òĩò FreeBSD Foundation.
ÐññéΥò áðù óéò èΥìáéò ð õñÕóáéò ìé ìðìßàð ÷ ñçóéììðñéìγíóáé áðù òĩòò éáóáóéãáóóðΥò ð òĩòò
ðñéçòΥò òĩòò áéá íá áéáéñññĩòĩ óá ðññíùííóá òĩòò éãñññíγíóáé ãìðñééÛ óγìãñē. ¼ðìò áóðΥò
ãìðñééñññĩóáé óá áóðù òĩ éãñññĩ éáé áéá ùóáð áðù áóðΥò ãññññéáé ç ììÛáá ÁíÛðððçò òĩò FreeBSD ùóé
áβιάé ðééáíñí íá áβιάé ãìðñééÛ óγìãñē, éá ááßòá Υία áðù óá óγìãñē: “TM” ð “®”.

Áóðù òĩ Ûñéññ ðññéãñÛóáé ðñò ìðññáßòá íá ñðéìßóáðá Υία ôåß÷ìò ðññíóôáóßàð (firewall) ÷ ñçóéììðñéìγíóáð
ìéá PPP óγìãñē ìΎúò òçäåöþññ òôĩ FreeBSD ìá òĩ IPFW. Ðéì óðáéãññéìΥία, ðññéãñÛóáé òç ñγéìéçò áññð
ôåß÷ìò ðññíóôáóßàð óá ìéá óγìãñē ìΎúò òçäåöþññ ðñò Υ÷áé ãññññéç IP áéãγéçñç. Áóðù òĩ éãñññĩ ãáí
áó÷ñéãñéáé ìá òĩ ðñò éá ñðéìßóáðá òçí ãñ÷éç óáð óγìãñē ìΎúò PPP. Áéá ðññéçóóñðññð ðéçñññññññ
ó÷áðééÛ ìá ðéð ñðéìßóáðò ìéáð óγìãñē ìΎúò PPP ááßòá òç óáéßáá ãññéááð ppp(8).

1 Ðññéññìò

Áóðù òĩ éãñññĩ ðññéãñÛóáé òçí áéáéééáóßá ðñò ÷ ññéÛéãóáé áéá íá ñðéìßóáðá Υία ôåß÷ìò ðññíóôáóßàð òôĩ
FreeBSD ùóáí ç IP áéãγéçñç ãññññé ãññññéÛ áðù òĩ ISP óáð. Ðáñññē ðñò Υ÷ù ðññíóðáéðóáé íá èÛñ áóðù òĩ
éãñññĩ ùóí òĩ ãñññññ ðéì ðñññð éáé óñóðù, áßòá ãðñññóááðñé íá óðáéãññ ðéð áéñññéçðáð, óá ó÷ñééá ð ðéð
ðññíóôáðò óáð òç áéãγéçñç òñò óðáãñáðΥία: <marcs@draenor.org>.

2 ÐáñÛñáðññé òñò ðñññía

Áéá íá ìðññΥóáðá íá ÷ ñçóéììðñéìγíóáðá òĩ IPFW, ðñññéáé íá áññññáðñóáðá òçí ó÷áðééç ðññíóðññéç òôñ ðñññía óáð.
Áéá ðññéçóóñðññð ðéçñññññññ ò÷áðééÛ ìá òç ìáðáéðððéç òñò ðñññía, ááßòá òĩ òñññ ñðéìßóáññ òñò ðñññía òôñ
Áã÷áéñññé (http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html). Éá ðñññéáé íá
ðñññéçóóáðá ðéð ðñññéÛ ðñññññ òóéð ñðéìßóáðò òñò ðñññía óáð áéá íá áññññññññ òçí ðññíóðññéç áéá òĩ
IPFW:

```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεεᾶ οᾶβ÷ἰοο δñιόοᾶόβαο οἰῶ δῶñΠία.

ΌγιαΒυός: Άόου οί έαβιαί έαυηάβ υόε Ύ÷ άόά άαέάόάόΠόάέ όγι Ύέαιός 5.X οίθ FreeBSD Π ιέα όεί όηύόόάό. Άί ÷ήόόείήίέαβόά όγι Ύέαιός 4.X, όύόά έά όηΎόάέ ίά άίάηάήίέΠόάόά όγι άόέέϊΆP *IPFW2* έάέ ίά άέάάΎόάόά ός όάέβάά άίΠεάέό ipfw(8) έέά όηέόόόύόόηάό όέόήϊήϊήβάό ό÷ άόέέΎ ίά όγι άόέέϊΆP *IPFW2*. ΠήϊόΎίόά έάέάβόάηά όϊ όϊΠιά *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFWALL_VERBOSE
```

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

```
options IPFWIREWALL_VERBOSE_LIMIT=500
```

[illegible]

```
options IPDIVER
```

Āíāñāīđīéāß ôá *divert* sockets, ðīō èà äīyīā āñāüōāñā ôé êŬīīōī.

[illegible]

3 ÁëéãÿÒ óôï /etc/rc.conf äéá íá öïñôþíáôáé ôï ôâß÷ìò
ðñïóôáóßàò

Ἄεά íá áíáñāīđīēáβōáé ôī ôāβ÷īō ðñīōōáōβáō éáōŬ ôçī áêēβīçōç ôīō ôōōōðīáōīō éáé áéá íá īñβōáōā ôī āñ÷āβī íā ôīōō éáíuíāō ôīō ôāβ÷īōō ðñīōōáōβáō, ðñÝðāé íá áīçīāñþróāō ôī āñ÷āβī /etc/rc.conf. ἌðēŬ ðñīōēÝōā ôēō ðāñāēŬōū āñāīÝð:

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

```
Ääå ðänëööüöñäño 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 “ðýçç”, 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_όγιάååçð"
```

Όçç èΎçç òìò ðñìððë_ðçð_όγιάååçð ðñÝðåé íå åÛëååå òì ùñå ççð óýìååðð ðåð, ùðò òì Ύ÷åå åðìççåýóåé óòì åñ÷åíìåå /etc/ppp/ppp.conf.

5 Ìé éåíüìåò òìò firewall

Όì ìññ ðìò åðñìÝíåç ðññå åβíåé íå ìñβòìåå òìò éåññåð òìò firewall. Ìé éåññåð òìò ìðìβìòð ðåñåñÛòììåå ååð åβíåé åñëåðÛ éåññ åéå òìòð ðåñåóóùðåñìòð ÷ñΠóóåå ìå dialup óýìååç, åëÛ ìýåå òðì÷ñåðéñ åβíåé, ìýåå åβíåé åðíååùì íå óåññÛåñìò ìå ðéð åñÛååð ùëù òùì ÷ñçóððì dialup. Ìðññìýì, ùùð, íå ÷ñçóëìåýóòì ùð Ύíå éåëù ðåñÛåååñå ðëèβòåùì òìò IPFW éåé åβíåé ó÷åðéÛ åýëëì íå òìòð ðñìóåñìùóååå óðéð åéÛð ðåð åñÛååð.

Áð åñ÷åíìåå ùùð ìå ðéð ååóééÛð åñ÷Ûð åññåóóý ðåβ÷ìòð ðñìóóåååå. ìå èëåóóù ðåβ÷ìòð ðñìóóåååå åðåññåýåé ååð’ åñ÷Πì èÛåå óýìååç. Ì åéå÷åñéóðð ìðññåé ýóóåñå íå ðñìéÝóåé éåññåð åéå íå äðéòñÝðåé ìññ óðååññåñìÝíåð óðíåÝóåé ìå ðåññÛíå åðù òì ðåβ÷ìòð ðñìóóåååå. Ç ðëì óðìçéóìΎìç óåññÛ òùì éåñññì óå Ύíå èëåóóù ðåβ÷ìòð åβíåé: ðñðåé ìé éåññåð ðìò äðéòñÝðìò ìåñéÛð óðíåÝóåð, éåé ðÝëì ìé éåññåð ðìò åðåññåýìò ìðìååððìåå Ûëçç óýìååç. Ç ëñåçð ðβòù åðù åðòù åβíåé ùé ðñðåé åÛåååå òìò éåññåð ðìò äðéòñÝðìò ðñÛåñåå íå ðåñÛòìò éåé ýóóåñå ùåå óå Ûëëå åðåññåýìíóåé åðòùìåå.

ΌðéÛìåå, ëëðùì, Ύíå éåðÛëñì óòì ìðìβì åå åðìççåýìíóåé ìé éåññåð òìò ðåβ÷ìòð ðñìóóåååå. Όå åðòù òì Ûñëñì ÷ñçóëìðìéýìå ùð ðåñÛåååñå òì éåðÛëñì /etc/firewall. ΆëëÛìåå éåðÛëñì ìΎóå óå åðòùì éåé åçìéìñåΠóóåå òì åñ÷åíìåå ðìò òì ùñÛ òìò åβ÷åñå åñÛåé óòì rc.conf. Όçñåçðåå ðùð ìðññååå íå åëëÛååå òì ùñå òìò åñ÷åíìåå åðòý óå ùé èΎååå. Áðòùð ì ìåçåð åβíåé åðòù òì ùñå óåñ ðåñÛåååñå éåé ìññ.

Áð åññåå ðññå Ύíå ðåñÛåååñå ðåβ÷ìòð ðñìóóåååå ìå åñëåðÛ åðåñçåçåðéÛ 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 ðëëçñüíΎíí óαβ÷ιò ðñüóóáóβáo, óì ðñíβì óóíaΎóáέó óóέó èýñáo 22 έάέ 80 έάέ έáoáñŮóάέ üέáo óέó Ůέέáo óóíaΎóáέó óôi áñ÷áβì έáoáññáoþò óìó óóóóþíaóìò. ÐēΎíí áβóóά Ύóìέíí έέά áðáíáέέβίçóç. Ůì óαβ÷ιò ðñüóóáóβáo έά áíáñáðñέçέáβ áóóüíáóά έάέ έά öìñóþóάέ óìòó έáíüíáo ðìó ðñíóέΎóάóά. Áí áá áβíάέ áóóü þ Ύ÷áoά ðñέάáþðìóá ðñíáέþíaóá, þ áí Ύ÷áoά èŮðñέáo ðñíóŮóáέó áέά íá áέíñèùέáβ áóóü óì Ůñèñí, áðέέíéíüíþóóά íάέβ ðìó íá email.

6 Άñùòþóάέò

1. ΆέΎðü ðçíýíáóά üðüò “limit 500 reached on entry 2800” έάέ íáoŮ áðü áóóü óì óýóóçìŮ ðìó óóáíáoŮάέ íá έáoáññŮóάέ óá ðάέΎóά ðìó áìðñáβæííóάέ áðü óì óαβ÷ιò ðñüóóáóβáo. Άìóέáýάέ áέüíá óì firewall ðìó;

Áóóü áðέŮ óçíaβíάέ ðüò Ύ÷άέ ðñçóέííðñέçέáβ óì ðΎάέóìí üñέí έáoáññáoþò (logging) áέά áóóü óìí έáíüíá. Ì έáíüíáo ð þáέìð áíáέíéíòέáβ íá áìóέáýάέ, áέέŮ ááí έά óóΎέíáέ ðέά ðçíýíáóά óôi áñ÷áβì έáoáññáoþò óìó óóóóþíaóìò ðΎ÷ñέ íá ðçááíþóáoðá ðŮέέ óìòð íáoñçóŮò. ðññáβóá íá ðçááíþóáoðá óìòð íáoñçóŮò ðá óçí áíóíēþ

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðìþóáðá òì ùñέì éάóάññáðòðò óóέò ñðèìβóάέò òìò ððñþíá óάò ìá όçì áðέέìāþ IPFWALL_VERBOSE_LIMIT ùðòð ðññέññÛðáì ðññάðÛñ. ìðññáβóá íá áέέÛíáðá áðóò òì ùñέì (÷ ùñβò íá ìáðáάέùòðβóáðá ðÛέέ òì ððñþíá óάò éάέ íá éÛíáðá reboot) ÷ ñçóέììðìέþíðáò όçì sysctl(8) όέìþ net.inet.ip.fw.verbose_limit.

2. ÊÛðìέì éÛέìò ðñÝðáέ íá Ýáέíá. Áέέìýέçóά óέò áíòìéÝð éάóÛ ãñÛìá éάέ όþñá éέάέäþέçéá áðÝñ.

Áðóòò ì ìäçäùð òðìéÝðáέ ùðέ ÷ ñçóέììðìέáβóá òì *userland-ppp*, áέ áðóò éέ ìé éáfííáð ðìò áβñíðáέ ÷ ñçóέììðìέìýì òì tun0 interface, ðìò áíðέóóìé÷ áβ óόçì ðñþόç óýíááόç ðìò óðέÛ÷ íáðáέ ìá òì ppp(8) (áέέέþð áñóóò éάέ ùð *user-ppp*). Ç áðñìáìç óýíááόç éá ÷ ñçóέììðìέìýóá òì tun1, ìáóÛ òì tun2 éάέ ðÛáέ éÝáñíðáð.

Éá ðñÝðáέ áðβόçò íá èòìÛóðá ùðέ òì pppd(8) ÷ ñçóέììðìέáβ òì interface ppp0, ìðòðá áí ìáέέìþóáðá όç óýíááόþ óάò ìá òì pppd(8) éá ðñÝðáέ íá áíðέéάóóðþóáðá òì tun0 ìá ppp0. ÐññάέÛóù éá ááβñìòìá Ýíá áýέìέì ðññðì íá áέέÛíáðá òìòò éáfííáð òìò firewall éάðÛέέçéá. 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 éάðáέÛááðá áí ÷ ñçóέììðìέáβóá òì ppp(8) þ òì pppd(8) ìðññáβóá íá áíáðÛóáðá όçì Ýñññì όçò ifconfig(8) áóìý áíáñññðìέçéáβ ç óýíááόþ óάò. Ð.÷., áέά ìéá óýíááόç ðìò áíáñññðìέþέçéá áðò òì pppd(8) éá ááβðá éÛóέ óáf áðóò (ááβ÷ñíðáέ ìñì ìé ó÷áðέέÝð ãñññìÝð):

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

Άðò όçì Ûέέç, áέά ìéá óýíááόç ðìò áíáñññðìέþέçéá ìá òì ppp(8) (*user-ppp*) èÛ ðññðá íá ááβðá éÛóέ ðññññέì ìá òì ðññάέÛóù:

```
% 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...)
```