

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÷õñùĩΥĩ ãìðñééÛ óγìãñĩ òĩò FreeBSD Foundation.
ÐñééΥò áðù óéò èΥìáéò ð õñÛóáéò ïé ïðĩßàò ÷ñçóéììðñééγìáé áðù òĩòò éáóáóéãáóóðΥò ð òĩòò
ðùéçðΥò òĩòò áéá íá áéáéñññĩ òá ðñĩùíííá òĩòò èàùññĩγìáé ãìðñééÛ óγìãñĩ. ¼ðìò áóðΥò
ãìðñééÛ óá áóðù òĩ èáβìãñĩ éáé áéá ùóáò áðù áóðΥò ãìðñééÛ ç ììÛáá ÁíÛðððçò òĩò FreeBSD ùóé
áβιάé ðééáííí íá áβιάé ãìðñééÛ óγìãñĩ, éá ááßòá Υία áðù òá óγìãñĩ: “TM” ð “®”.

Áóðù òĩ Ûñéñ ðñééãñÛóáé ðùò ïðñãßòá íá ðñéßóáòá Υία ôåß÷ìò ðñĩóðáóßàò (firewall) ÷ñçóéììðñééγìáé
íéá PPP óγìãñĩ ΙΎού όçäåöþñĩ òôĩ FreeBSD íá òĩ IPFW. Ðéí óðéãéñéñĩΥία, ðñééãñÛóáé òç ñγéìéç ãìðò
ôåß÷ìò ðñĩóðáóßàò óá íéá óγìãñĩ ΙΎού όçäåöþñĩ ðìò Υ÷áé ãñíãñéç IP áéãýðçíç. Áóðù òĩ èáβìãñĩ ããí
áó÷ñéãßóáé íá òĩ ðùò éá ðñéßóáòá òçí ãñ÷éç óáò óγìãñĩ ΙΎού PPP. Áéá ðñééóóóðñãò ðéçññññßàò
ó÷áðééÛ íá ðéò ðñéßóáéò íéáò óγìãñĩ ΙΎού PPP ááßòá òç óáéßáá ãñðéááð ppp(8).

1 Ðñüéñĩò

Áóðù òĩ èáβìãñĩ ðñééãñÛóáé òçí áéáéééáóßá ðìò ÷ñééÛéáóáé áéá íá ðñéßóáòá Υία ôåß÷ìò ðñĩóðáóßàò òôĩ
FreeBSD ùóáí ç IP áéãýðçíç ãβìáóáé ãñíãñééÛ áðù òĩ ISP óáò. Ðáññéñ ðìò Υ÷ù ðñĩóðáéðóáé íá èÛñ áóðù òĩ
èáβìãñĩ ùóí òĩ ãñíãñéñ ðéí ðéðñãò éáé óùóðù, ááßòá ãðññóááðéé íá óðáßéãáò ðéò áéññéðóáéò, óá ó÷üééá ð ðéò
ðññóóáéò óáò òç áéãýðçíç òìò óðããñãóΥία: <marcs@draenor.org>.

2 ÐáñÛìáðñĩé òĩò ððññía

Áéá íá ïðñΥóáòá íá ÷ñçóéììðñééγìáé òĩ IPFW, ðñΥðáé íá áíóùíáððóáòá òçí ó÷áðééç ððñññéç òôñ ððññía óáò.
Áéá ðñééóóóðñãò ðéçññññßàò ó÷áðééÛ íá òç ìáðáéðððéç òìò ððññía, ááßòá òĩ òìñ ðñéßóáùí òìò ððññía òôñ
Áã÷áéññáéí (http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html). Éá ðñΥðáé íá
ðññééγóáòá ðéò ðñééãñÛò ãðééñãóðéò ðñéßóáéò òìò ððññía óáò áéá íá áññãññéðóáòá òçí ððñññéç áéá òĩ
IPFW:

```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεεᾶ οᾶβ÷ἰοο δñιόοᾶόβαο οἰῶ δῶñΠία.

ΌγίαΒυός: Άόου όι έαβιαί έαυηάβ υόε Ύ÷ άόά άαέάόάόΠόάέ όγι Ύέαιός 5.X όιό FreeBSD Π ιέα όεί όηύόόάός. Αί ÷ήόόείόίόιέαβόά όγι Ύέαιός 4.X, όυόά έα όηΎόάέ ίά άίάηάίόίέΠόάόά όγι άόέέϊΆΠ *IPFW2* έάέ ίά άέάάΎόάόά ός όάέβΆά άίΠεάέό ipfw(8) έέά όαήέόόύόόαήάό όέόηίόίήβάό ό÷ άόέέΎ ίά όγι άόέέϊΆΠ *IPFW2*. ΠήιόΎίόά έάέάβόάήά όι όίΠιά *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 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"
```

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 ΑίóύìáòùìΎìç ìåðÛññåç Äéåðëýíóåùì óìò PPP

Άέά íá äðéõñÝðååå óå Ûëëá ìç÷áííååå òìò äééðýìò óåå íá óðíåÝííóåé ìå òìì Ýìù èùòì ìΎóù òìò FreeBSD, ÷ñçóëìðìéðíóåå òì ùð “ðýëç”, åå ðñÝðåé íá áíñññìðìéΠóóåå ôçí ΑίóύìáòùìΎìç ìåðÛññåç äéåðëýíóåùì òìò PPP (NAT). Άέά íá åbíåé áðòù, ðñìéÝóåå óòì áñ÷åí /etc/rc.conf ðéð ðåñåÛòù åñåñìÝð:

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

Όόç èΎóç òìò ðñìððë_ðçð_όγιάαός ðñÝðåé íá åÛëååå òì ùññå ççð óýíååðð óåð, ùðòò òì Ύ÷ååå äðìçëåýóåé óòì áñ÷åí /etc/ppp/ppp.conf.

5 Ìé éåíüíåò óìò firewall

Όì ìññ ðìò äðñÝíåé ðññå åbíåé íá ìñβóìñå òìò éåññåð òìò firewall. Ìé éåññåð òìò ìðìβìòð ðåñéåñÛòìñå ååð åbíåé åñëåðÛ éåññ åéá òìòð ðåñéóóùðåñìòð ÷ñΠóóåå ìå dialup óýíååç, äëëÛ ìýåå òðì÷ñåðéñ åbíåé, ìýåå åbíåé äóñååùì íá óåññÛåñì ìå ðéð áñÛååð ùëù òùì ÷ñçóðñí dialup. Ìðññýí, ùñð, íá ÷ñçóëñåýóòì ùð Ύíå éåëù ðåñÛåéåñå ðññåååå òìò IPFW éåé åbíåé ó÷åðéëÛ åýëëì íá òìòð ðñìóåññåååå óééð äéëÝð óåð áñÛååð.

Áð áñ÷βóìñå ùñð ìå ðéð ååóéëÝð áñ÷Ýð áññð èëåóóòý óåβ÷ìòð ðñìóóåååå. ìå èëåóóòù óåβ÷ìò ðñìóóåååå äååññåýå éåð’ áñ÷Πí èÛëå óýíååç. Ì åéá÷åñéóóðð ìðññåé ýóóåñå íá ðñìéÝóåé éåññåð åéá íá äðéõñÝðåé ìññ óåååññåññÝíåð óðíåÝóåé íá ðåññÛíå äðù òì óåβ÷ìòð ðñìóóåååå. Ç ðëì óðìçééóìΎìç óåññÛ òùì éåññññ óå Ύíå èëåóóòù óåβ÷ìò åbíåé: ðñðåé ìé éåññåð ðìò äðéõñÝðìò ìåñéëÝð óðíåÝóåð, éåé ðÝëì ìé éåññåð ðìò äðåññåýíìò ìðìåååððìå Ûëçç óýíååç. Ç ëñåçëð ðβòù äðù áðòù åbíåé ùé ðñðåé åÛåååå òìò éåññåð ðìò äðéõñÝðìò ðñÛåñåå íá ðåñÛòìò éåé ýóóåñå ùëå óå Ûëëå äðåññåýííóåé áðòùñåå.

ΌðéÛìå, ëëðùì, Ύíå éåðÛëññ óòì ìðìβì éå äðìçëåýííóåé ìé éåññåð òìò óåβ÷ìòð ðñìóóåååå. Όå áðòù òì Ûñëññ ÷ñçóëìðìéýíå ùð ðåñÛåéåñå òì éåðÛëññ /etc/firewall. ΆëëÛìå éåðÛëññ ìΎóå óå áðòù éåé åçìéìñåΠóóå òì áñ÷åí fwrules ðìò òì ùññÛ òìò åβ÷åñ åñÛåé óòì rc.conf. ΌçñåéΠóå ðùð ìðññååå íá åëëÛñåå òì ùññå òìò áñ÷åñ ððìò óå ùé èΎëåå. Áðòù ì ìåçåð åbíåé áðòù òì ùññå óåñ ðåñÛåéåñå éåé ìññ.

Áð åññå ðññå Ύíå ðåñÛåéåñå óåβ÷ìòð ðñìóóåååå ìå åñëåðÛ äðåñçåñåéëÛ 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 icmp types 0,3,8,11,12

# Deny and log all the rest.
$fwcmd add deny log ip from any to any
```

Όþñá Ý÷áoá Ýία ðεεçñùιÝιí ðάβ÷ιò ðñïóóáóβáo, ðι ιðιβι óðíaÝóáέð óðέð εýñáo 22 έάέ 80 έάέ έáoáñÛóáέ ùέáo óέð Ûέέáo óðíaÝóáέð óôi áñ÷άβι έáoáññáoðò ðιò óóóðßáoιò. ÐεÝιí άβóóά Ýðιειιέ áέα άðáíáέέβιçóç. Όι ðάβ÷ιò ðñïóóáóβáo έá áíáñáðιεçέάβ áóðuiáoά έάέ έá ðιñóþáoέ ðιòð έáíuiáo ðιò ðñιóέÝóáoά. Áί άá άβíáέ áóðu ð Ý÷áoά ιðιεάáððιòά ðñíáεßáoά, ð áί Ý÷áoά εÛðιεáo ðñιòÛóáέð áέα íá áειñεùέάβ áóðu ðι Ûñèñι, áðέειρεíuißóóά íáεβ ιιò íá email.

6 Άñùòþáoέò

1. ΆεÝðù ιçíýíáoά ùðùð “limit 500 reached on entry 2800” έάέ íáoÛ áðu áóðu ðι óýóðçìÛ ιιò óðáíáoÛάέ íá έáoáññÛóáέ óá ðáεÝóά ðιò άιðñáβειíóáέ áðu ðι ðάβ÷ιò ðñïóóáóβáo. Άιòέáýáέ áέuiά ðι firewall ιιò;

Áóðu áðεÛ óçíáβíáέ ðùð Ý÷άε ðñóέιιðιεçέάβ ðι ιÝάέóðι ùñέι έáoáññáoðò (logging) áέα áóðu ðι έáíuiά. Ì έáíuiáoð ιßάειð áíáειρεíòεάβ íá áιòέáýáέ, áεεÛ ááí έá óóÝειíáέ ðέα ιçíýíáoά óôi áñ÷άβι έáoáññáoðò ðιò óóóðßáoιò ιÝ÷ñέ íá ιçáííßóáoά ðÛέέ ðιòð íáðñçðÝð. Ìðñíáβóά íá ιçáííßóáoά ðιòð íáðñçðÝð íá ðçí áιðιεð

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðñáóáðá òñ ùñéñ éáóáññáöðò óóέò ñöèìβóáέò òñ ðññá íá óáo ìá όçñ áðέέñáð IPFWALL_VERBOSE_LIMIT ùðòð ðññéññÛðáì ðññáðÛñ. ìðññáβóá íá áέέÛñáðá áðóó òñ ùñéñ (÷ ùñβò íá ìáðááèòóóβóáðá ðÛέέ òñ ðññá íá óáo éάέ íá èÛñáðá reboot) ÷ ñçóέññðñéñíðáo όçñ sysctl(8) όέìð net.inet.ip.fw.verbose_limit.

2. ÈÛðñéñ èÛèò ðñÝðáé íá Ýáéíá. Áέñéýçóá óέò áñòñéÝð éáoÛ ãñÛñá éάέ όþñá èèáέäþèçéá áðÝñ.

Áðóóò ì ìäçäùð òðñéÝðáé ùóέ ÷ ñçóέññðñéáβóá òñ *userland-ppp*, áé áðóó èé ìé éáfñíáð ðñò áβññíóáé ÷ ñçóέññðñéñýñ òñ tun0 interface, ðñò áíóέóóñé÷ áβ óόçñ ðñþόç óýñááόç ðñò óóέÛ÷ íáðáé ìá òñ ppp(8) (áέέέðò áñóóó èάέ ùò *user-ppp*). Ç áðñíáñç óýñááόç éá ÷ ñçóέññðñéñýóá òñ tun1, ìáðÛ òñ tun2 éάέ ðÛáé èÝáññóáo.

Èá ðñÝðáé áðβόçò íá èòìÛóðá ùóέ òñ pppd(8) ÷ ñçóέññðñéáβ òñ interface ppp0, ìðóðá áñ ìáέέñáóáðá όç óýñááόð óáo ìá òñ pppd(8) éá ðñÝðáé íá áíóέéáóáóóðáðá òñ tun0 ìá ppp0. ÐññáéÛóó èá ááβññóñá Ýñá áýέññ ðññðññ íá áέέÛñáðá òñòò éáfñíáð òñò firewall éáoðÛέçéá. ìé áñ÷έέñβ éáfñíáð όþññíóáé óá Ýñá áñ÷áβñ 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 éáðáéÛááðá áñ ÷ ñçóέññðñéáβóá òñ ppp(8) þ òñ pppd(8) ìðññáβóá íá áñáðÛóáðá όçñ Ýññññ όçò ifconfig(8) áóñý áññññðñéçéáβ ç óýñááόð óáo. Ð.÷., áέá ìéá óýñááόç ðñò áññññðñéçéçéá áðñ òñ pppd(8) éá ááβðá èÛóέ óáñ áðóó (ááβ÷ññóáé ìññ ìé ó÷áðέéÝð ãññññÝð):

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

Άðñ όçñ Ûέçç, áέá ìéá óýñááόç ðñò áññññðñéçéçéá ìá òñ ppp(8) (*user-ppp*) èÛ ðññðñá íá ááβðá èÛóέ ðñññññéñ ìá òñ ðññáéÛóó:

```
% 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...)
```