

Όγιάαός ΙΎού Όçäåöþñĩõ êáé Ôåß÷ĩò 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÷õñùĩΥĩĩ àìðñééÛ óγìáĩēĩ ôĩõ FreeBSD Foundation.
ÐñēēΥò áðù óéò ēΥìáéò ð õñÛóáéò ïé ïðĩßàò ÷ ñçóéìĩðñēĩγìóáé áðù ôĩõò éáóáóéäóáóòΥò ð ôĩõò
ðñēçòΥò ôĩõò áéá íá áéáēñβĩĩôĩ óá ðñĩùũĩóá ôĩõò èàùññĩγìóáé àìðñééÛ óγìáĩēá. ¼ðĩò áóòΥò
àìðáíβæĩìóáé óá áóòù ôĩ èáβìáñĩ éáé áéá ùóáò áðù áóòΥò àìùñβæáé ç ììÛáá ÁíÛðòðĩçò ôĩõ FreeBSD ùóé
åβìáé ðééáìĩ íá áβìáé àìðñééÛ óγìáĩēá, éá åáßòå Υία áðù óá óγìáĩēá: “TM” ð “®”.

Áóòù ôĩ Ûñēñĩ ðåñéåñÛóáé ðùò ïðñåßòå íá ñðēĩßóåðå Υία ôåß÷ĩò ðñĩóðáóßàò (firewall) ÷ ñçóéìĩðñēĩγìóáò
ìéá PPP óγìááóç ìΎóù òçäåöþñĩõ óôĩ FreeBSD ìå ôĩ IPFW. Ðéĩ óðææåñēĩΥία, ðåñéåñÛóáé òç ñγέìéóç áìùð
ôåß÷ĩò ðñĩóðáóßàò óá ìéá óγìááóç ìΎóù òçäåöþñĩõ ðñĩ Õ÷áé äóíáíéēð IP áéåγέðĩóç. Áóòù ôĩ èáβìáñĩ åáí
áó÷ñæåßóáé ìå ôĩ ðùò éå ñðēĩßóåðå òçí áñ÷éēð óáð óγìááóç ìΎóù PPP. Áéá ðåñéóóùðåñåð ðéçññĩõñβåð
ó÷åðééÛ ìå ðéò ñðēĩßóåðò ìéáð óγìááóç ìΎóù PPP ååßòå òç óåßååå ãñðéåéáð ppp(8).

1 Ðñüēĩāĩò

Áóòù ôĩ èáβìáñĩ ðåñéåñÛóáé òçí áéåæééáóßå ðñĩ ÷ ñåéÛæåðáé áéá íá ñðēĩßóåðå Υία ôåß÷ĩò ðñĩóðáóßàò óôĩ
FreeBSD ùðáí ç IP áéåγέðĩóç åβìáðáé äóíáíééÛ áðù ôĩ ISP óáð. Ðåññüēĩ ðñĩ Õ÷÷ ðñĩóðåðóáé íá èÛñ áóòù ôĩ
èáβìáñĩ ùóĩ ôĩ äóíáðùĩ ðéĩ ðēðñåð éáé óùóòù, åáßòå äððñüóååðñé íá óðåßæåðå ðéò æéññèðóáéð, óá ó÷üééá ð ðéò
ðñĩòÛóáéð óáð óòç áéåγέðĩóç ôĩõ óðååñåðΥá: <marcs@draenor.org>.

2 ÐåñÛìåðñĩé ôĩõ ððñĩá

Áéá íá ìðñΥóåðå íá ÷ ñçóéìĩðñēĩγìóáð ôĩ IPFW, ðñΥðåé íá áìóùìåðóåðå òçí ó÷åðéēð ððñĩóðñēĩç óôĩ ððñĩá óáð.
Áéá ðåñéóóùðåñåð ðéçññĩõñβåð ó÷åðééÛ ìå òç ìåðåðððéóç ôĩõ ððñĩá, ååßòå ôĩ ðñĩá ñðēĩßóåðò ôĩõ ððñĩá óôĩ
Åå÷åññåéĩ (http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html). Éå ðñΥðåé íá
ðñĩóéΥóåðå ðéò ðåñåéÛò ððéññΥò óðéò ñðēĩßóåðò ôĩõ ððñĩá óáð áéá íá áñåñåðñéðóåðå òçí ððñĩóðñēĩç áéá ôĩ
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 όηύόόάό. Άί ÷ όηόέίόίόιέαβόά όγι Ύέαιός 4.X, όυόά έα όηΎόάέ ίά άίάηάίόίέΠόάόά όγι άόέέίάΠ *IPFW2* έάέ ίά άέάάΎόάόά ός όάέβάά άίΠεάέό ipfw(8) έέά όαήέόόύόόαήάό όέγνιόιήβάό ό÷ άόέέΎ ίά όγι άόέέίάΠ *IPFW2*. ΌήιόΎίόά 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 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. ἌðēŨ ðñīōēŸōā ôēō ðāñāēŨōū āñāīŸō:

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

Àéá ðàíéóóúðàñàò ðëçñröivñBàò ó-âôêêÛ ià ôç ôçíáóBàò êáèáìéÛò áðu áòòÝò èèò àñànÝò, ñBíòá íèá íáôêÛ óóí /etc/default/rc.conf éáé áéááÛ00ðá ôçí man óäèBää rc.conf(5)

4 ΆíññìðìéΠόοά όçí ΑίούìάòùìΎίç ìάòÛñάός Äéäðéýíóáùì όìò PPP

Άέά íá äðéòñÝðáòá óá Ûεéá ìç÷áíΠíáóá όìò äééóýìò óáò íá óóíáΎííóáé ìá όìí Ύíù éùóìí ìΎóù όìò FreeBSD, ÷ñçóéìðìéÞíóáò όì ùò “ðýεç”, éá ðñÝðáé íá áíñññìðìéΠόóáò όçí ΑίούìάòùìΎίç ìάòÛñάός äéäðéýíóáùì όìò PPP (NAT). Άέά íá áβíáé áòòù, ðñìóéΎóóá óòì áñ÷áβì /etc/rc.conf óéò ðáñáéÛòù áñáñΎò:

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

Όόç èΎόç όìò ðñìòβē_όçò_όγíäáόçò ðñÝðáé íá áÛéäòá όì ùíñá όçò óýíäáóðò óáò, ùòòù όì Ύ÷äòá áðìεçéäýóáé óòì áñ÷áβì /etc/ppp/ppp.conf.

5 Ìé éáíüíäò όìò firewall

Όì ùíñ όìò áðñΎíáé όÞñá áβíáé íá ìñβóìòìá όìòð éáíüíäò όìò firewall. Ìé éáíüíäò όìòð ìðìβìòð ðáñéáñÛóìòìá äáÞ áβíáé áñéäòÛ éáéìβ áéá όìòð ðáñéóóùòáñìòð ÷ñΠóóáò ìá dialup óýíäáόç, äééÛ ìýóá óðì÷ñáùóééìβ áβíáé, ìýóá áβíáé äóíáòùì íá óáéñéÛæìòì ìá óéò áíÛäéäò ùéùì óùì ÷ñçóóÞí dialup. Ìðìñíýí, ùìòð, íá ÷ñçóéìäýóìòì ùò Ύíá éáéù ðáñÛäáéäìá ñòéìβóáùì όìò IPFW éáé áβíáé ó÷äóééÛ áýéìèí íá όìòð ðñìóáñìüóáòá óóéò äééΎò óáò áíÛäéäò.

Áò áñ÷βóìòìá ùìòð ìá óéò äáóééΎò áñ÷Ύò áíüò éäéóóóíý óáβ÷ìòð ðñìóóáóáò. Íá éäéóóóù óáβ÷ìò ðñìóóáóáò ääáññáýáé éáò’ áñ÷Þí éÛéä óýíäáόç. Ì áéá÷áéñéóóðò ìðìñáβ ýóóáñá íá ðñìóéΎóáé éáíüíäò áéá íá äðéòñÝðáé ùíñ óóäéäéñéíΎíáò óóíáΎóáéò íá ðáñíÛíá áðù όì óáβ÷ìò ðñìóóáóáò. Ç ðéí óðìçééóìΎίç óáéñÛ óùì éáíüíüí óá Ύíá éäéóóóù óáβ÷ìò áβíáé: ðñÞóá ìé éáíüíäò όìò äðéòñÝðìòì ìáñééΎò óóíáΎóáéò, éáé óΎéìò ìé éáíüíäò όìò äðáññáýíòì ìðìéäáÞðìòá Ûéçç óýíäáόç. Ç εíäéεÞ ðβóù áðù áòòù áβíáé ùóé ðñÞóá áÛæáòá όìòð éáíüíäò όìò äðéòñÝðìòì ðñÛáíáóá íá ðáñÛóìòì éáé ýóóáñá ùéá óá Ûεéá äðáññáýííóáé áòòùìáóá.

ΌðéÛìòá, εíéðùí, Ύíá éáòÛéìáí óóìí ìðìβì éá áðìεçéäýííóáé ìé éáíüíäò όìò óáβ÷ìòð ðñìóóáóáò. Óá áòòù όì Ûñéññ ÷ñçóéìðìéíýíá ùò ðáñÛäáéäìá όìí éáòÛéìáí /etc/firewall. ΆééÛìòá éáòÛéìáí ìΎóá óá áòòùì éáé äçìéìòñáΠóóá όì áñ÷áβì fwrules όìò όì ùíñÛ όìò áβ÷áíá áñÛðáé óòì rc.conf. ΌçìäéÞóóá ðùò ìðìñáβóá íá äééÛíäòá όì ùíñá όìò áñ÷áβìò áòòíý óá ùóé èΎéäòá. Áòòùò ì ìäçäùò áβíáé áòòù όì ùíñá óáí ðáñÛäáéäìá éáé ùíñ.

Áò äíýíá όÞñá Ύíá ðáñÛäáéäìá óáβ÷ìòð ðñìóóáóáò ìá áñéäòÛ äðáíçäçíáóééÛ ó÷úééá.

```
# 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 Ύía ðēēçñüíΎíí óαβ÷ιò ðñüóóáóβáo, ðí ðñíβí óñíaΎóáέò óóέò éýñáo 22 έάέ 80 έάέ έáoáñŰóáέ üέáo óέò Üέέáo óñíaΎóáέò óôi áñ÷áβí έáoáññáoþò ðιò óóóðñíaóιò. ÐēΎíí áβóóá Ύóιέιιέ áέá áðáíáέέβίçóç. Όι óαβ÷ιò ðñüóóáóβáo έá áíáñáñðιέçέáβ áóóüíáóá έάέ έá öñóþóáέ ðιò έáíüíáo ðιò ðñιόέΎóáóá. Áí áá áβíáέ áóóü þ Ύ÷áoá ðιέέáþðιòá ðñíáέñíaóá, þ áí Ύ÷áoá έÜðιέáo ðñιòŰóáέò áέá íá áέíñέúέáβ áóóü ðι Üñèñí, áðέέιέíüíþóóá íáέβ ðιò íá email.

6 Άñùòþóáέò

1. ΆέΎðü ðçíýíáóá üðüò “limit 500 reached on entry 2800” έάέ íáoŰ áðü áóóü ðι óýóóçíŰ ðιò óóáíáoŰάέ íá έáoáñŰóáέ óá ðáέΎóá ðιò áñðíáβæííóáέ áðü ðι óαβ÷ιò ðñüóóáóβáo. Άñέáyáέ áέüíá ðι firewall ðιò;

Áóóü áðέŰ óçíáβíáέ ðüò Ύ÷áέ ðñçóέíñðιέçέáβ ðι ðΎάέóðι üñέí έáoáññáoþò (logging) áέá áóóü ðι έáíüíá. Ì έáíüíáo ðι þáέιð áíáέιíέòέáβ íá áñέáyáέ, áέέŰ ááí έá óóΎέíáέ ðέá ðçíýíáóá óôi áñ÷áβí έáoáññáoþò ðιò óóóðñíaóιò ðΎ÷ñέ íá ðçáíñβóáoá ðŰέέ ðιò ðáñçóŰò. ðññáβóá íá ðçáíñβóáoá ðιò ðáñçóŰò ðι ðçí áíñέþ

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðñáóáðá òì ùñéì éáóáññáðòðò óóέò ñðèìβóáέò òìò ððñáíá óáo ìá òçí áðέέñáð IPFWALL_VERBOSE_LIMIT ùðòð ðáñέáñÛðáì ðáñáðÛñ. Ìðññáβóá íá áέέÛíáðá áðóó òì ùñéì (÷ ùñβò íá ìáðááèòóðβóáðá ðÛέέ òì ððñáíá óáo éάέ íá èÛíáðá reboot) ÷ ñçóέììðñéíáð òçí sysctl(8) óéìð net.inet.ip.fw.verbose_limit.

2. ÈÛðñéì èÛèò ðñÝðáé íá Ýáέíá. Áέñéýçóá óέò áíóñéÝð éáoÛ ãñÛíá éάέ òþñá èéáέäþèçéá áðÝñ.

Áðóóò ì ìäçáùð òðñéÝðáé ùðé ÷ ñçóέììðñéáβóá òì *userland-ppp*, áé áðóó èé ìé éáfííáð ðìò áβñíóáé ÷ ñçóέììðñéíýì òì tun0 interface, ðìò áíóέóðñé÷ áβ òçí ðñþòç óýíááóç ðìò òðéÛ÷ íáðáé ìá òì ppp(8) (áέέèðð áñóóó èάέ ùð *user-ppp*). Ç áðñíáíç óýíááóç éá ÷ ñçóέììðñéíýóá òì tun1, ìáðÛ òì tun2 éάέ ðÛáé èÝáñíóáð.

Èá ðñÝðáé áðβóçò íá èòìÛóðá ùðé òì pppd(8) ÷ ñçóέììðñéáβ òì interface ppp0, ìðóðá áí ìáέέñáóáðá òç óýíááóð óáo ìá òì pppd(8) éá ðñÝðáé íá áíóέéáóáóðβóáðá òì tun0 ìá ppp0. ÐáñáéÛóó èá ááβñíðìá Ýíá áýέñéì ðññðñí íá áέέÛíáðá òìòð éáfííáð òìò firewall éáoðÛέçéá. Ìé áñ÷έέìβ éáfííáð òþáñíóáé 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
```

Άέá íá éáðáéÛááðá áí ÷ ñçóέììðñéáβóá òì ppp(8) þ òì pppd(8) ìðññáβóá íá áñáðÛóáðá òçí Ýññáì òçð ifconfig(8) áóñý áñáñáñðñéçéáβ ç óýíááóð óáo. Ð.÷., áέá ìéá óýíááóç ðìò áñáñáñðñéçéá áðñ òì pppd(8) éá ááβðá èÛóέ óáí áðóó (ááβ÷ñíðáé ìññ ìé ò÷áðééÝð ãñáñÝð):

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

Άðñ òçí Ûέçç, áέá ìéá óýíááóç ðìò áñáñáñðñéçéá ìá òì ppp(8) (*user-ppp*) èÛ ðñáðá íá ááβðá èÛóέ ðáñññéí ìá òì ðáñáéÛóó:

```
% 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...)
```