

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 ÷ ñçóéììðñēĩγìóáé áðù ôĩõò éáóáóéäåóáóðΥò ð ôĩõò
ðñēçôΥò ôĩõò áéá íá áéáēñßñĩôĩ óá ðñĩùũĩóá ôĩõò èàùññĩγìóáé àìðñééÛ óγìáĩēá. ¼ðñò áóðΥò
àìðáíßæñĩóáé óá áðù òĩ èáßìáñĩ éáé áéá ùóáò áðù áóðΥò àìùñßæáé ç ììÛáá ÁíÛððçĩçò ôĩõ FreeBSD ùóé
åβιάέ ðééáìíĩ íá áβιάέ àìðñééÛ óγìáĩēá, éá åáßðá Υία áðù óá óγìáĩēá: “TM” ð “®”.

Áðù òĩ Ûñēñĩ ðáñéáñÛóáé ðñò ïðñåßðá íá ñðēĩßóáðá Υία ôåß÷ĩò ðñĩóðáóßàò (firewall) ÷ ñçóéììðñēĩγìóáò
ìéá PPP óγìááóç ìΎúò òçäåöþñĩõ óôĩ FreeBSD ìá ôĩ IPFW. Ðéĩ óðäēäēñēĩΥία, ðáñéáñÛóáé çç ñγēìéóç áìùð
ôåß÷ĩò ðñĩóðáóßàò óá ìéá óγìááóç ìΎúò òçäåöþñĩõ ðñò Υ÷áé äóĩáíéēð IP áéáγēðçĩç. Áðù òĩ èáßìáñĩ äáí
áó÷ñēåßðáé ìá ôĩ ðñò éá ñðēĩßóáðá ççĩ áñ÷éēð óáð óγìááóç ìΎúò PPP. Áéá ðáñéóóùðáñáð ðççññĩõñßàð
ó÷áðéēÛ ìá ðéð ñðēĩßóáéð ìéáð óγìááóç ìΎúò PPP åáßðá çç óåßßáá àñðéäéáð ppp(8).

1 Ðññēĩñĩò

Áðù òĩ èáßìáñĩ ðáñéáñÛóáé ççĩ áéáéééáóßá ðñò ÷ ñáéÛæáóáé áéá íá ñðēĩßóáðá Υία ôåß÷ĩò ðñĩóðáóßàò óôĩ
FreeBSD ùðáí ç IP áéáγēðçĩç äßíáðáé äóĩáíéēÛ áðù ôĩ ISP óáð. Ðáññēē ðñò Υ÷ù ðñĩóðáéðóáé íá èÛñ áðù òĩ
èáßìáñĩ ùóĩ ôĩ äóĩáðñĩ ðéĩ ðēðñáð éáé óùóðù, åáßðá äððñùóáäððñé íá óðåßäðá ðéð äéññēðóáéð, óá ó÷ñēéá ð ðéð
ðññòÛóáéð óáð óçç áéáγēðçĩç ôñò óðáññáðΥá: <marcs@draenor.org>.

2 ÐáñÛìáðññé ôñò ððññía

Áéá íá ìðñΥóáðá íá ÷ ñçóéììðñēĩγìóáðá ôĩ IPFW, ðñΥðáé íá áìóùìáððóáðá ççĩ ó÷áðéēð ððñóðññēĩç óôĩ ððññía óáð.
Áéá ðáñéóóùðáñáð ðççññĩõñßàð ó÷áðéēÛ ìá çç ìáðáäēðððéóç ôñò ððññía, åáßðá ôĩ òññía ñðēĩßóáñĩ ôñò ððññía óôĩ
Áã÷áññáéĩ (http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html). Éá ðñΥðáé íá
ðññééΥóáðá ðéð ðáñáéÛðù äðéēñáΥð óðéð ñðēĩßóáéð ôñò ððññía óáð áéá íá áññáñññēĩγìóáðá ççĩ ððñóðññēĩç áéá ôĩ
IPFW:

4 ΆíññìðìéΠóóå ôçí ΆíóùìáòùìÝíç ìåðÛññåç Äéåðëýíóåùì òìò PPP

Άέά íå äðéòñÝðååå óå Ûëëå ìç÷åíìååå òìò äééðýìò óåå íå óñíåÝìíóåé ìå òìì Ýìù èùòì ìÝóù òìò FreeBSD, ÷ñçóëìðìéðìååå òì ùð “ðýëç”, åå ðñÝðåé íå áíñññìðìéΠóóåå ôçí áíóùìáòùìÝíç ìåðÛññåç äéåðëýíóåùì òìò PPP (NAT). Άέå íå åβίåé áðòù, ðñìéÝóåå óòì åñ÷åíìåå /etc/rc.conf ðéð ðåñåÛòù åñåñìÝð:

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

Όçç èÝóç òìò ðñìððë_ðçð_όγιάαόςçð ðñÝðåé íå åÛëååå òì ùñåå ççð óýìååððð óåð, ùðòù òì Ý÷ååå äðìççåýóåé óòì åñ÷åíìåå /etc/ppp/ppp.conf.

5 Ìé éåíñìåò òìò firewall

Όì ìññì ðìò äðñìÝíåé ðññå åβίåé íå ìñβòìåå òìò éåñìåå òìò firewall. Ìé éåñìåå òìò ìðìβìòð ðåñåñÛòììåå ååð åβίåé åñëåðÛ éåñìåé åéå òìòð ðåñåóóùðåñìòð ÷ñΠóóåå ìå dialup óýìååç, åëëÛ ìýåå òðì÷åñåéìå åβίåé, ìýåå åβίåé åóíååùì íå óåñëÛåñìò ìå ðéð åñÛååð ùëù òùì ÷ñçóððì dialup. ÌðñìÝí, ùìð, íå ÷ñçóëìåýóòì ùð Ýíå éåëù ðåñÛåéåñìå ðñìððåùì òìò IPFW éåé åβίåé ó÷åéåÛ åýëììé íå òìòð ðñìóåñìùóååå óééð åéëÝð óåð åñÛååð.

Áð åñ÷åñìåå ùìð ìå ðéð ååóéëÝð åñ÷åñìåå åñìð ðñìððåååð. Íå åëåóóùð ðåβ÷ìò ðñìóóåååð åðåññåýåé ååð’ åñ÷åñìåå óýìååç. Ì åéå÷åñåóðð ìðññåé ýóóåñå íå ðñìéÝóåé éåñìåå åéå íå äðéòñÝðåé ìññì óåååñåñåñìÝíåå óñíåÝóåé íå ðåñìÛíå åðù òì ðåβ÷ìò ðñìóóåååð. Ç ðëì óðìççéóìÝíç óåñÛ òùì éåñìåå óå Ýíå åëåóóùð ðåβ÷ìò åβίåé: ðñðåé ìé éåñìåå ðìò äðéòñÝðìò ìåñéëÝð óñíåÝóåé, éåé ðÝëì ìé éåñìåå ðìò äðåññåýìò ìðìååððìåå Ûëçç óýìååç. Ç ëñåçëð ðβòù åðù åðòù åβίåé ùéé ðñðåé åÛåååå òìò éåñìåå ðìò äðéòñÝðìò ðñÛåñåå íå ðåñÛòìò éåé ýóóåñå ùåå óå Ûëëå äðåññåýìíóåé åðòùìåå.

ΌðéÛìåå, ëëðùì, Ýíå éåðÛëñì óòì ìðìβì éå äðìççåýìíóåé ìé éåñìåå òìò ðåβ÷ìò ðñìóóåååð. Óå åðòù òì Ûñëñì ÷ñçóëìðìéýìå ùð ðåñÛåéåñìå òì éåðÛëñì /etc/firewall. ΆëëÛìåå éåðÛëñì ìÝóå óå åðòù éåé åçìéìñåΠóóåå òì åñ÷åñìåå fwrules ðìò òì ùñìÛ òìò åβ÷åñìå åñÛåé óòì rc.conf. Óçìåçðåå ðùð ìðññååå íå åëëÛååå òì ùñåå òìò åñ÷åñìåå åðòì ýéååå. Áðòùð ì ìåçåð åβίåé åðòù òì ùñåå óåñ ðåñÛåéåñìå éåé ìññì.

Áð åñýìå ðññå Ýíå ðåñÛåéåñìå ðåβ÷ìò ðñìóóåååð ìå åñëåðÛ äðåñçåçìååÛ ó÷åéå.

```
# 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 ðēēçñùíΎíí ðåβ÷ìð ðñïóóóβáð, ðí ðñβí óñíaΎóáéð óðéð èýñåð 22 éáé 80 éáé éáoáñÛóåé ùēåð óéð Ûēēåð óñíaΎóáéð óôi åñ÷åβí éáoáññáoðð ðñð óðóðβíáðñð. ÐēΎíí åβóðå Ύðñēñē áéá åðáñēēβíçç. Ôí ðåβ÷ìð ðñïóóóβáð éå áñåñññēçēåβ áððñíáðå éáé éå ðññóðåé ðñð éåñññð ðñð ðññóēΎóáðå. Áí åå åβñåé áððñ ð Ύ÷áoå ðññéååðññåð ðññåβñíáðå, ð åí Ύ÷áoå èÛðñéåð ðñññóóáéð áéá íå áéññēñēåβ áððñ ðí Ûññññ, åðéññēñññóðå íåæβ ðñð íå email.

6 Åññôðóåéð

1. ÅēΎðñ ðçññíáðå ùðñð limit 500 reached on entry 2800 éáé ðåðÛ áððñ ðí óýóðçìÛ ðñð óðñíåðÛåé íå éáoáññÛóåé ðå ðåēΎóå ðñð åñðñåñññóåé áððñ ðí ðåβ÷ìð ðññóóóβáð. Åññēåýåé åéññå ðí firewall ðñð;

Áððñ áðñÛ óçññññå ðñð Ύ÷åé ðñçóéññññçēåβ ðí ðΎåóðñ ùñññ éáoáñññáoðð (logging) áéá áððñ ðññ éåñññå. Ì éåñññåð ð ðåñð åñåññññåβ íå åññēåýåé, åēÛ ååñ éå óðΎññå ðéå ðçññíáðå óôi åñ÷åβí éáoáñññáoðð ðñð óðóðβíáðñð ðΎ÷ñé íå ðçåñññóóåð ðÛēé ðñð ðåññçðΎð. Ìðññåðå íå ðçåñññóóåð ðñð ðåññçðΎð ðå ðçññññññ

```
# 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 áðòò òì ùñέì (÷ ùñβò íá ìáðáάέùòòβóáðá 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. Áέìέìýçóά óέò áíòìέÝð éάóÛ ãñÛìá éάέ όþñá éέάέäþççéá áðÝñ.

Άðòòò ì ìäçäùð òðìέÝðáέ ùðέ ÷ ñçóέììðìέáβóá òì *userland-ppp*, áέ áðòò éέ ìέ éáfííáð ðìò áβñíðáέ ÷ ñçóέììðìέìýì òì tun0 interface, ðìò áíðέóóìέ÷ áβ óόçì ðñþόç óýíááόç ðìò óðέÛ÷ íáðáέ ìá òì ppp(8) (áέέέþð áñóðòò éάέ ùð *user-ppp*). Ç áðùìáìç óýíááόç éά ÷ ñçóέììðìέìýìóá òì tun1, ìáðÛ 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 áíðέéάóáóóþóáðá òì tun0 ìá ppp0. ÐññάέÛòù éá ááβñìòìá Ýíá áýέìέì ðñùðì íá áέέÛíáðá òìòò éáfííáð òìò firewall éάðÛέççéá. Ìέ 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 Ýñìäì όçò ifconfig(8) áóìý áíáññäìðìέççéá ç óýíááόþ óάò. Ð.÷., áέά ìέá óýíááόç ðìò áíáññäìðìέþççéá áðù òì pppd(8) éá ááβðá éÛóέ óáf áðòò (ááβ÷ñíðáέ ìùì ìέ ó÷áðέέÝð ãñáñìÝð):

```
% 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 Ûέçç, áέά ìέá óýíááόç ðìò áíáññäìðìέþççéá ìá òì ppp(8) (*user-ppp*) èÛ ðññðá íá ááβðá éÛóέ ðáññììέì ìá òì ðññάέÛòù:

```
% 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...)
```