

# 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.  
ÐñēéΥò áðù óéò èΥìáéò ð õñÛóáéò ïé ïðĩßàð ÷ ñçóéììðñēìγìóáé áðù òĩòò éáóáóéãáóóðΥò ð òĩòò  
ðñéçòΥò òĩòò áéá íá áéáéñññĩòĩ óá ðñĩùìíóá òĩòò èáùññĩγìóáé ãìðñééÛ óγìãñē. ¼ðìò áóðΥò  
ãìðáíβæìíóáé óá áóðù òĩ èáβìãñĩ éáé áéá ùóáð áðù áóðΥò ãìùññæáé ç ììÛáá ÁíÛðððĩçò òĩò FreeBSD ùóé  
åβιάé ðééáíìí íá áβιάé ãìðñééÛ óγìãñē, éá åáßðá Υία áðù óá óγìãñē: “TM” ð “®”.

Áóðù òĩ Ûñéññ ðãñéãñÛóáé ðñò ìðñãßðá íá ñðèìßóáðá Υία ôåß÷ìò ðñĩóðáóßàð (firewall) ÷ ñçóéììðñēìγìóáð  
ìéá PPP óγìãñēç ìΎóù òçäåöþñĩò óôĩ FreeBSD ìá òĩ IPFW. Ðéì óðãéãñéçìΥία, ðãñéãñÛóáé çç ñγéìéçç áíùð  
ôåß÷ìò ðñĩóðáóßàð óá ìéá óγìãñēç ìΎóù òçäåöþñĩò ðìò Υ÷áé ãñíãñéçç IP áéãýðñĩç. Áóðù òĩ èáβìãñĩ ããí  
áó÷ìãßðáé ìá òĩ ðñò éá ñðèìßóáðá ççí ãñ÷éçç óáð óγìãñēç ìΎóù PPP. Áéá ðãñéççóóðãñãð ðéçññĩññßàð  
ó÷ãðééÛ ìá ðéð ñðèìßóáéð ìéáð óγìãñēç ìΎóù PPP åáßðá çç óãñßáá ãñðéãáð ppp(8).

## 1 Ðññēñĩò

Áóðù òĩ èáβìãñĩ ðãñéãñÛóáé ççí áéãáééáóßá ðìò ÷ ñáéÛæáóáé áéá íá ñðèìßóáðá Υία ôåß÷ìò ðñĩóðáóßàð óôĩ  
FreeBSD ùðáí ç IP áéãýðñĩç ãβíáðáé ãñíãñééÛ áðù òĩ ISP óáð. Ðãññēñ ðìò Υ÷ù ðñĩóðáéðóáé íá èÛù áóðù òĩ  
èáβìãñĩ ùóí òĩ ãñíãññ ðéì ðéðñãð éáé óùóðù, åáßðá ãððññóáãðñé íá óðãñéãðá ðéð áéññèðóáéð, óá ó÷ùééá ð ðéð  
ðññòÛóáéð óáð óçç áéãýðñĩç òĩò óðããñãóΥá: <marcs@draenor.org>.

## 2 ÐãñÛíãññé òĩò ððññíá

Áéá íá ìðñΥóáðá íá ÷ ñçóéììðñēìγìóáðá òĩ IPFW, ðñΥðáé íá áíóóìãððóáðá ççí ó÷ãðééç ððññóðññéçç óôĩ ððññíá óáð.  
Áéá ðãñéççóóðãñãð ðéçññĩññßàð ó÷ãðééÛ ìá çç ìáðáãñððéçç òìò ððññíá, åáßðá òĩ òìñíá ñðèìßóáñ òìò ððññíá óôĩ  
Ãã÷áéñßáéñ ([http://www.FreeBSD.org/doc/el\\_GR.ISO8859-7/books/handbook/kernelconfig.html](http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html)). Éá ðñΥðáé íá  
ðññéççóóðãñãð ðéð ðãñéãñÛò ãðéçñññ òéð ñðèìßóáéð òìò ððññíá óáð áéá íá áíãñãññéççóáðá ççí ððññóðññéçç áéá òĩ  
IPFW:

```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεεᾶ οᾶβ÷ἰοο δñἰοᾶόβαο οἰῶ δῶñΠία.

**ΌγίαΒυός:** Άόου όι έαβιαί έαυηάβ υόε Ύ÷ άόά άαέάόάόόΠόάε όγι Ύέαιός 5.X όιό FreeBSD Π ιέα όεί όηύόόάό. Άί ÷ όηόόίόίέάβόά όγι Ύέαιός 4.X, όύόά έά όηΎόάε ίά άίάηάίόίέΠόάόά όγι άόέέϊΆ *IPFW2* έάέ ίά άέάάΎόάόά ός όάέβάά άίΠεάέό ipfw(8) έέά όαήέόόύόόάηά όέόηίόίηβάό ό÷ άόέέΎ ίά όγι άόέέϊΆ *IPFW2*. ΠηίόΎίόά έάέάβόάηά όι όίΠιά *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFWALL VERBOSE
```

ÓôÝéíáé ôá ìçíýíáôá äéá ôá éáoÜëëçéá ðáéÝôá óôi log ôiõ óõóôÞíáôîð.

```
options IPFIREWALL VERBOSE LIMIT=500
```

Ἄϋααε εὐϋιεῖ νηεῖ ὁδεὸ νινῤο θῖο εὐϋιεά αααῆαοP εα εαὸαανῤοαὸαε. ὃοε ἰθῖηαβὸα ἰά εαὸαανῤοαὸα ὁά ἰςῖῖαὸα αῖυ ὅῖ ὁαβ÷ῖθ θῖηῖοαὸαβὸ ÷ῖηβὸ ὅῖ εβῖαῖῖ ἰά ααἰβὸῖῖ ὁά αῖ÷ῖα εαὸααῆαοP ὁῖο ὁῖοῖPαῖαὸυ ὁά ἰα αα÷ῖαβὸα εὐϋιεά αῖβεαὸς. Ὅῖ νηεῖ 500 ἰςῖῖῖῤοῖ αβῖάε ἰεά αῆεαὸῤ εῖαεεP ὀειP, αεεῤ ἰθῖηαβὸα ἰά θῖῖοαῖῖῤοαὸα αὸῖP ὀςῖ ὀειP ἰῖῖῖῖῖ ἰά ὀεὸ αῖαεὸPῖαεὸ ὅῖο αεεῖῖ ὁά αεεὸῖῖ.

```
options IPDIVER
```

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

[illegible]

3 ÁëëáÑò óôi /etc/rc.conf ãéá íá öĩñôþíáôáé ôĩ ôâß÷ìò  
ðñĩóôáóßàò

Ἄεά íá áíáñāīđīēáβōáé ôī ôāβ÷īō ðñīōōáōβāō éáōŬ ôçī áēēβīçōç ôīō ôōōōðīáōīō éáé áéá íá īñβōāōā ôī āñ÷āβī íā ôīōō éáíuíāō ôīō ôāβ÷īōō ðñīōōáōβāō, ðñŶđāé íá áīçīāñþróāōā ôī āñ÷āβī /etc/rc.conf. ἌðēŬ ðñīōēŶōā ôēō ðāñāēŬōū āñāīŶð:

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

Àéá ðàíéóóúðàñàò ðëçñröivñBàò ó-àòéèÛ ià ôç öçíáóBàò éáéäíéÙò áðu áòòÝò óéò àñànÝò, ñBìòá íéá íáóéÛ óöí /etc/defaults/rc.conf éáé äéääÛÓòá ôçí man óäèBää rc.conf(5)

## 4 ΆíññìðìέΠóòά όçí ΑίóύìáòùìΎίç ìáòÛññάόç Äέáðēýíóáùì óìò PPP

Άέά íá áðέòñÝòáòά óá Ûέέá ìç÷áíΠíáóá όìò áέέóýìò óáò íá óóíáΎííóáέ ìá όìí Ύíù έùóìí ìΎóù όìò FreeBSD, ÷ñçóέìíðìέΠíóáò όì ùò “ðýέç”, έá ðñÝðáέ íá áíñññìðìέΠóòά όçí ΑίóύìáòùìΎίç ìáòÛññάόç äέáðēýíóáùì όìò PPP (NAT). Άέά íá áβíáέ áòòù, ðñìóέΎóáά όóì áñ÷áβì /etc/rc.conf óέò ðáñáέÛòù áñáñΎò:

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

Όόç èΎόç όìò ðñìòβέ\_όçò\_όγíááόçò ðñÝðáέ íá áÛέáòά όì ùíñά όçò óγíááóΠò óáò, ùòòù όì Ύ÷áòά áðìέçέáýóáέ óóì áñ÷áβì /etc/ppp/ppp.conf.

## 5 Ìέ έáíüíáò όìò firewall

Όì ùíñ όìò áðñΎíáέ όΠñά áβíáέ íá ìñβóìòìá όìò έáíüíáò όìò firewall. Ìέ έáíüíáò όìò ìðìβìòð ðáñέáñÛóìòìá ááΠ áβíáέ áñέáòÛ έáέìβ áέá όìòð ðáñέóóùòáñìòð ÷ñΠóóáò ìá dialup óγíááόç, áέέÛ ìýóá όðì÷ñáùóέέìβ áβíáέ, ìýóá áβíáέ áóíáòùì íá óáέñέÛέìòì íá óέò áíÛáέáò ùέùì óùì ÷ñçóóΠí dialup. Ìðìñíýí, ùìòð, íá ÷ñçóέìáýóìòì ùò Ύíá έáέù ðáñÛááέáìá ñòέìβóáùì όìò IPFW έáέ áβíáέ ó÷áòέέÛ áýέìì íá όìòð ðñìóáñìüóáòά óóέò áέέΎò óáò áíÛáέáò.

Áò áñ÷βóìòìá ùìòð ìá óέò ááóέέΎò áñ÷Ύò áíüò έέáέóóíý óáβ÷ìòð ðñìóóáóáò. Íá έέáέóóù óáβ÷ìò ðñìóóáóáò áðááññáýáέ έáò’ áñ÷Πí έÛέá óγíááόç. Ì áέá÷áέñέóóΠò ìðìñáβ ýóóáñά íá ðñìóέΎóáέ έáíüíáò áέá íá áðέòñÝòáέ ìüñ óóáέáñέñέΎíáò óóíáΎóáέò íá ðáñíÛíá áðù όì óáβ÷ìò ðñìóóáóáò. Ç ðέì óóìçέέóìΎίç óáέñÛ óùì έáíüñí óá Ύíá έέáέóóù óáβ÷ìò áβíáέ: ðñΠóá ìέ έáíüíáò όìò áðέòñÝòìòì ìáñέέΎò óóíáΎóáέò, έáέ óÝέìò ìέ έáíüíáò όìò áðááññáýíòì ìðìέááΠðìòά Ûέέç óγíááόç. Ç έìáέέΠ ðβóù áðù áòòù áβíáέ ùóέ ðñΠóá áÛááòά όìòð έáíüíáò όìò áðέòñÝòìòì ðñÛáíáóá íá ðáñÛóìòì έáέ ýóóáñά ùέá óá Ûέέá áðááññáýííóáέ áòòùìáóá.

ΌóέÛìòά, έìέðùí, Ύíá έáòÛέìáì óóìí ìðìβì έá áðìέçέáýííóáέ ìέ έáíüíáò όìò óáβ÷ìòð ðñìóóáóáò. Óá áòòù όì Ûñέññ ÷ñçóέìíðìέíýíá ùò ðáñÛááέáìá όìí έáòÛέìáì /etc/firewall. ΆέέÛìòά έáòÛέìáì ìΎóá óá áòòùì έáέ äçìέìòñáΠóóá όì áñ÷áβì fwrules όìò όì ùíñÛ όìò áβ÷áìá áñÛóáέ óóì rc.conf. ÓçìáέΠóóá ðùò ìðìñáβóá íá áέέÛíáòά όì ùíñά όìò áñ÷áβìò áòòíý óá ùóέ èΎέáòά. Áòòùò ì ìáçáùò áβíáέ áòòù όì ùíñά óáí ðáñÛááέáìá έáέ ìüñ.

Áò äíýíá όΠñά Ύíá ðáñÛááέáìá óáβ÷ìòð ðñìóóáóáò ìá áñέáòÛ áðáíçáçíáóέέÛ ó÷έέá.

```
# 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
```

Όπná Ý÷áoá Ýía ðēēçñüíÝíí óåβ÷ìò ðñüóóáóβáo, òì ìðìβì óðíaÝóáéoð óóéo èýñáo 22 éáé 80 éáé éáoáñÜöáé üēáo óéo Üēēáo óðíaÝóáéoð óôi áñ÷åβì éáoáñáoðò òìò óóóðβíaóìò. ÐēÝíí åβóðå Ýðìēñē áéá åðáíæēβίçóc. Ôì óåβ÷ìò ðñüóóáóβáo éå áíåññðēçēåβ áóðüíáoá éáé éå òñòðóå òìò éáíüíáo ðìò ðñìóēÝóáoå. Áí åå åβíæé áóðü Þ Ý÷áoå ððēéåððìòå ðññæβíaóå, Þ áí Ý÷áoå èÜðēéáo ðñìÜóáéoð áéá íå áéññēèéåβ áóðü òì Üñēñì, åðēēñēñìðóóå íææβ ììò íå email.

## 6 ÅñùòÞóáéoò

1. ÅēÝðü ìçíýíáoå üðüò limit 500 reached on entry 2800 éáé íåðÜ áðü áóðü òì óýóóçìÜ ììò óðáíáoÜå íå éáoáñÜöáé óå ðåÝóå ðìò åìðñæñíóåé áðü òì óåβ÷ìò ðñüóóáóβáo. Åìçåýåé áéñüå òì firewall ììò;

Áóðü áðēÜ óçíåβíæé ðüò Ý÷æé ðñçóēññðēçēåβ òì ìÝæéóòì ùñēñ éáoáñáoðò (logging) áéá áóðü òì éáíüíå. Ì éáíüíå ì βæìò áíæññòēåβ íå ðìçåýåé, áēēÜ ååñ éå óóÝñíæé ðéå ìçíýíáoå óôi áñ÷åβì éáoáñáoðò òìò óóóðβíaóìò ìÝ÷ñé íå ìçåñíóóåðå ðÜēé òìò ìåñçóÝò. Ìðñåβóå íå ìçåñíóóåðå òìò ìåñçóÝò ìå òçííññÞ

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáßóá íá áõìßóáóá òì ùñéì éáóáññáößò óóéò ñöèìßóáέò òìò ðöñßíá óáò ìá òçì áðéëíäß IPFWALL\_VERBOSE\_LIMIT ùðòò ðññéññÛðáì ðññáðÛñ. ìðññáßóá íá áέέÛíáóá áóòò òì ùñéì (÷ ùñßò íá ìáóáäèòóóßóáò ðÛέέ òì ðöñßíá óáò éάέ íá èÛíáóá reboot) ÷ ñçóéììðéííóáò òçì sysctl(8) óéìß net.inet.ip.fw.verbose\_limit.

2. ÈÛðéì èÛèò ðñÝðáé íá Ýáéíá. Áéëéýçóá óéò áíóñéÝò éáóÛ ãñÛíá éάέ òþñá èéáéäþççéá áðÝñ.

Áóòòò ì ìäçäùò òðñéÝðáé ùóé ÷ ñçóéììðéíáßóá òì *userland-ppp*, áé áóòò èé ìé éáfííáò ðìò äßñíóáé ÷ ñçóéììðéíéýì òì tun0 interface, ðìò áíóéóóé÷÷ äß óóçì ðñþòç óýíááóç ðìò óóéÛ÷ íáóáé ìá òì ppp(8) (áééëþò áñóòò éάέ ùò *user-ppp*). Ç áðñíáíç óýíááóç éá ÷ ñçóéììðéíéýóá òì tun1, ìáóÛ òì tun2 éάέ ðÛáé èÝáñíóáò.

Èá ðñÝðáé áðßóçò íá èòìÛóóá ùóé òì pppd(8) ÷ ñçóéììðéíáß òì interface ppp0, ìðòòá áí ìáέéíßóáóá òç óýíááóß óáò ìá òì pppd(8) éá ðñÝðáé íá áíóééáóáóóßóáò òì tun0 ìá ppp0. ÐññáéÛòò éá ääßñíóá Ýíá áýéëè ðññðì íá áέéÛíáóá òìòò éáfííáò òìò firewall éáðÛέççéá. ìé áñ÷ééìß éáfííáò òþæííóáé óá Ýíá áñ÷äß 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 éáóáéÛááóá áí ÷ ñçóéììðéíáßóá òì ppp(8) ð òì pppd(8) ìðññáßóá íá áñáóÛóáóá òçì Ýññäì òçò ifconfig(8) áóñý áñññäñðéççéä ç óýíááóß óáò. Ð.÷., áέá ìéá óýíááóç ðìò áñññäñðéççéä áðò òì pppd(8) éá ääßóá èÛóé óáf áóòò (ääß÷ñíóáé ìñì ìé ò÷äóééÝò ãñññÝò):

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

Άðò òçì Ûέçç, áέá ìéá óýíááóç ðìò áñññäñðéççéä ìá òì ppp(8) (*user-ppp*) èÛ ðññðá íá ääßóá èÛóé ðññññéì ìá òì ðññáéÛòò:

```
% 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...)
```