

# 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 ïðĩßàð ÷ ñçóéìĩðñēĩγìóáé áðù ôĩõò éáóáóéäåóáóðΥò ð ôĩõò  
ðñēçðΥò ôĩõò áéá íá äéáēñßñĩôĩ óá ðñĩùũíóá ôĩõò èàùññĩγìóáé àìðñééÛ óγìáĩēá. ¼ðĩò áóðΥò  
àìðáíßæñĩóáé óá áðù òĩ èáßìáñĩ éáé áéá ùóáð áðù áóðΥò àìùñßæáé ç ììÛáá ÁíÛððõçò ôĩõ FreeBSD ùóé  
åβιάé ðééáíũí íá áβιάé àìðñééÛ óγìáĩēá, éá åáßðá Υία áðù óá óγìáĩēá: “TM” ð “®”.

Áðù òĩ Ûñēñĩ ðñéñāñÛóáé ðùð ïðñāßðá íá ñðēĩßóáðá Υία ôåß÷ĩò ðñĩóðáóßàð (firewall) ÷ ñçóéìĩðñēĩγìóáð  
ìéá PPP óγìááç ìΎúò òçäåöþñĩõ óôĩ FreeBSD ìá ôĩ IPFW. Ðéĩ óðäēäēñēĩΥία, ðñéñāñÛóáé ç ñγēìéçç áñùð  
ôåß÷ĩò ðñĩóðáóßàð óá ìéá óγìááç ìΎúò òçäåöþñĩõ ðñĩ Õ÷áé äñíáíēē IP äéäγēðĩç. Áðù òĩ èáßìáñĩ äáí  
áç÷ñēåßðáé ìá ôĩ ðùð éá ñðēĩßóáðá ççí áñ÷ēēð óáð óγìááç ìΎúò PPP. Áéá ðñéçóóùðñāð ðççññĩõñßàð  
ó÷áðéēÛ ìá ðéð ñðēĩßóáðò ìéáð óγìááç ìΎúò PPP åáßðá çç óåßåá äñðéäéáð ppp(8).

## 1 Ðññēĩñĩò

Áðù òĩ èáßìáñĩ ðñéñāñÛóáé ççí äéäéééáóßá ðñĩ ÷ñāéÛæåóáé áéá íá ñðēĩßóáðá Υία ôåß÷ĩò ðñĩóðáóßàð óôĩ  
FreeBSD ùðáí ç IP äéäγēðĩçç äßñáðáé äñíáíēēÛ áðù ôĩ ISP óáð. Ðáñññēĩ ðñĩ Õ÷÷ ðñĩóðáéðóáé íá èÛñ áðù òĩ  
èáßìáñĩ ùóĩ ôĩ äñíáðñĩ ðéĩ ðēðñāð éáé óùóðù, åáßðá äððññóåäðñē íá óðåßäðá ðéð äéññēðóáðò, óá ó÷ñēéá ð ðéð  
ðññòÛóáðò óáð óçç äéäγēðĩçç ôñĩ óðāññāðΥá: <marcs@draenor.org>.

## 2 ÐáñÛìáðññē ôñĩ ððññía

Áéá íá ìðñΥóáðá íá ÷ ñçóéìĩðñēĩγìóáðá ôĩ IPFW, ðñΥðáé íá áíóùìáððóáðá ççí ó÷áðéēð ððñóðññēĩç óôĩ ððññía óáð.  
Áéá ðñéçóóùðñāð ðççññĩõñßàð ó÷áðéēÛ ìá çç ìáðāæðððéçç ôñĩ ððññía, åáßðá ôĩ òññía ñðēĩßóáñĩ ôñĩ ððññía óôĩ  
Åā÷äēñßäēĩ ([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  
ðññéçΥóáðá ðéð ðññāéÛð ððéññāΥð óðéð ñðēĩßóáðò ôñĩ ððññía óáð áéá íá áññāññēðñóáðá ççí ððñóðññēĩç áéá ôĩ  
IPFW:

```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεεᾶ οᾶβ÷ἰοο δñἰοᾶόβαο οἰῶ δῶñΠία.

**ΌγίαΒυός:** Άδου οι έαβιαί έαυηάβ υός Ύ÷ άόά άάέάόάόΡόάέ όγι Ύέαιρός 5.X οιό FreeBSD Ρ ιέα όεί όηύόόάό. Άί ÷ όγείόίόίέαβόά όγι Ύέαιρός 4.X, όύόά έά όηΎόάέ ίά άίάηάίόίέΡόάόά όγι άόέέίάΡ *IPFW2* έάέ ίά άέάάΎόάόά όγ όάέβάά άίΡεάέό ipfw(8) έέά όηέόόόύόόηάό όέγνίόίόηβάό ό÷ άόέέΎ ίά όγι άόέέίάΡ *IPFW2*. όηίόΎίόά έάέάβόάηά όί όίΡιά *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFWALL VERBOSE
```

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

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

[illegible]

```
options IPDIVERT
```

Āīāñāīōīēāß ôā *divert* sockets, ðīō èā āīyīā āñāūōāñā ôē ēŪīīōī.

**Ἐν ἡμετέροις τόποις:** Ἰουεὸ οὐδ' ἀπαρροαδοῖα ἰὰ θεοὺ πτολεβορεοῦ ἐσέ οὗσι ἰαδαᾶπερ ποθεός οἱ το δὲ πρία οἷο ἵφι ἐβῆ ἰαδα  
ἀδαίσεθις; Αἱ ἐβῆ ἰαδα ἀδαίσεθις; οἱ αὐτοὶ οἱ οὗσι παρὶ ἰδιναρ ἰα ἐσέ αὐτὰρ βιοῖα ἀδ' ὅτι οὐ γινώσκουσιν οἱ αὐτοί.  
Ἐν τῇ δεξιᾷ ἰα παρὶ τῇ ἰα ἰα ἀπαρροαδοῖα ἰα ἐσέ ἰα οἱ το παρ-τοῦ δὲ πτολεβορεοῦ ἐσέ ἰα ἀγία κηρύξαι ὑμᾶς οἱ  
οὐδ' ἀπαρροαδοῖα ἰα παρὶ τῇ ἰα πτολεβορεοῦ.

3 ÁëéãÑò óòì /etc/rc.conf ãéá íá öĩñôþíáôáé ôĩ ôâß÷ìò  
ðñĩóôáóßàò

Ἄεά íá áíáñāīđīēáβōáé ôī ôāβ÷īō ðñīōōáōβáō ēáoŬ ôçí âēēβíçōç ôīō ôōōōðīáōīō ēáé áéá íá īñβōáōā ôī āñ÷āβī íā ôīōō ēáíuíāō ôīō ôāβ÷īōō ðñīōōáōβáō, ðñÝðāé íá áíçíāñþróāō ôī āñ÷āβī /etc/rc.conf. ἌðēŬ ðñīōēÝōā ôēō ðāñāēŬōū āñāīÝð:

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

Àéá ðàíéóóúðàñàò ðëçñröivñBäò ó-äòéèÛ iä ôç öçíáóBäò éäéäíéÙò äðu äòðÝò èéò àñànÝò, ñBíôä íéä íáééÛ óöí /etc/defaults/rc.conf éäé äéääÛÖðä ôçí man óäëBää rc.conf(5)

## 4 ΆíññìðìέΠóòά όçí ΑίóύìáòùìΎίç ìáòÛññάόç Äέáðēýíóáùì óìò PPP

Άέά íá áðέòñÝòáòά óá Ûέέá ìç÷áíΠíáòά òìò áέέóýìò óáò íá óòíáΎííóáέ ìá òìí Ύíù έùóìí ìΎóù òìò FreeBSD, ÷ñçóέììðìέΠíóáò òì ùò “ðýέç”, έá ðñÝðáέ íá áíñññìðìέΠóòά όçí ΑίóύìáòùìΎίç ìáòÛññάόç äέáðēýíóáùì òìò PPP (NAT). Άέά íá áβíáέ áòòù, ðñìóέΎóóά óòì áñ÷áβì /etc/rc.conf óέò ðáñáέÛòù áñáñΎò:

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

Όόç èΎόç òìò ðñìòβέ\_òçò\_όγíááόçò ðñÝðáέ íá áÛέáòά òì ùíñά όçò óýíááóΠò óáò, ùòòù òì Ύ÷áòά áðìέçέáýóáέ óòì áñ÷áβì /etc/ppp/ppp.conf.

## 5 Ìέ έáíüíáò òìò firewall

Όì ìüñ ðìò áðñΎíáέ òΠñά áβíáέ íá ìñβóìòìá òìò έáíüíáò òìò firewall. Ìέ έáíüíáò òìò ìðìβìòð ðáñέáñÛòìòìá ááΠ áβíáέ áñέáòÛ έáέìβ áέá òìòð ðáñέóóùòáñìòð ÷ñΠóóáò ìá dialup óýíááόç, áέέÛ ìýóά òðì÷ñáùóέέìβ áβíáέ, ìýóά áβíáέ áòíáòùì íá óáέñέÛέìòì íá óέò áíÛáέáò ùέùì òùì ÷ñçóòΠí dialup. Ìðìñíýí, ùìò, íá ÷ñçóέìáýóìòì ùò Ύíá έáέù ðáñÛááέáìá ñòέìβóáùì òìò IPFW έáέ áβíáέ ó÷áòέέÛ áýέìèí íá òìòð ðñìóáñìüóáòά óóέò áέέΎò óáò áíÛáέáò.

Áò áñ÷βóìòìá ùìò ìá óέò ááóέέΎò áñ÷Ύò áíüò έέáέóòìý óáβ÷ìòð ðñìóóáóáò. Íá έέáέóóù óáβ÷ìò ðñìóóáóáò áðááññáýáέ έáò’ áñ÷Πí έÛέá óýíááόç. Ì áέá÷áέñέóóð ìðìñáβ ýóóáñά íá ðñìóέΎóáέ έáíüíáò áέá íá áðέòñÝòáέ ìüñ óóáέáñέñéΎíáò óòíáΎóáέò íá ðáñíÛíá áðù òì óáβ÷ìò ðñìóóáóáò. Ç ðéí óòìçέέóìΎίç óáέñÛ òùì έáíüíüí óá Ύíá έέáέóóù óáβ÷ìò áβíáέ: ðñΠóά ìέ έáíüíáò ðìò áðέòñÝðìòì ìáñέέΎò óòíáΎóáέò, έáέ òΎέìò ìέ έáíüíáò ðìò áðááññáýìòì ìðìέááΠðìòά Ûέέç óýíááόç. Ç έìáέέΠ ðβóù áðù áòòù áβíáέ ùóέ ðñΠóά áÛέáòά òìò έáíüíáò ðìò áðέòñÝðìòì ðñÛáíáòά íá ðáñÛóìòì έáέ ýóóáñά ùέá óá Ûέέá áðááññáýííóáέ áòòùìáóά.

ΌóέÛìòά, έìέðüí, Ύíá έáòÛέìáí óòìí ìðìβì έá áðìέçέáýííóáέ ìέ έáíüíáò òìò óáβ÷ìòð ðñìóóáóáò. Όά áòòù òì Ûñέññ ÷ñçóέììðìέíýíá ùò ðáñÛááέáìá òìí έáòÛέìáí /etc/firewall. ΆέέÛìòά έáòÛέìáí ìΎóά óá áòòùí έáέ äçìέìòñáΠóóά òì áñ÷áβì fwrules ðìò òì ùíñÛ òìò áβ÷áìá áñÛóáέ óòì rc.conf. ΌçìáέΠóóά ðùò ìðìñáβóά íá áέέÛíáòά òì ùíñά òìò áñ÷áβìò áòòìý óá ùóέ èΎέáòά. Áòòùò ì ìäçáùò áβíáέ áòòù òì ùíñά óáí ðáñÛááέáìá έáέ ìüñ.

Áò äíýíá òΠñά Ύíá ðáñÛááέáìá óáβ÷ìòð ðñìóóáóáò ìá áñέáòÛ áðáíçäçíáóέέÛ 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 icmp types 0,3,8,11,12

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

Όþñá Ϊ÷áðá Ϊíá ðëëçññùΪñ ðåβ÷ìò ðñüóóáóßáò, ðì ðñßì óñíáΪóáéð óðéð èýñåð 22 éáé 80 éáé éáðáñÛöåé ùëåð óéð Ûëëåð óñíáΪóáéð óõï åñ÷åßì éáðáññåððò ðñò óðóðßíáðñò. ÐëΪñ åßóðå Ϊðñëñé áéá åðáíåëëßççç. Ôì ðåβ÷ìò ðñüóóáóßáò éå áíåññðñéçéåß áððñíáðá éáé éå ðññðóåé ðñò éåññíåð ðñò ðññóëΪóáðå. Áí åå åßíåé áððñ ð Ϊ÷áðå ððñéååððñå ðññåßíáðå, ð áí Ϊ÷áðå èÛðñéåð ðññòÛóáéð áéá íå áéññëñååß áððñ ðñ Ûñëññ, åðéçñëñññóðå íåæß ðñò ðå email.

## 6 Åñùòßóåéò

1. ÅëΪðñ ðçññíáðå ùðñò “limit 500 reached on entry 2800” éáé ðåðÛ áðñ áððñ ðñ óýóðçÛ ðñò óðáíåðÛåé íå éåðáññÛöåé ðå ðåëΪóå ðñò åñðñåñññóåé áðñ ðñ ðåβ÷ìò ðñüóóáóßáò. Åñçåýåé áéññå ðñ firewall ðñò;

Áððñ áðëÛ óçñåßíåé ðñò Ϊ÷å ðñçóéññðñéçéåß ðñ ðΪåóðñ ùñëñ éåðáññåððò (logging) áéá áððñ ðñ éåññíå. Ì éåññíåð ðñ ðåñð áñåñññóåß íå åñçåýåé, áëëÛ ååñ éå óðΪçñåé ðéå ðçññíáðå óõï åñ÷åßì éåðáññåððò ðñò óðóðßíáðñò ðΪ÷ñé íå ðçåññóáðå ðÛéé ðñò ðåñççðΪð. Ìðñåßðå íå ðçåññóáðå ðñò ðåñççðΪð ðå ðçñ áñññð

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðñáóáóá òì ùñéì éáóáññáöðò óóέò ñòèìβóáέò òìò ðòñáíá óáo ìá όçí áðέέìáÐ IPFWALL\_VERBOSE\_LIMIT ùðòò ðáñέáñÛðáìá ðáñáðÛñ. Ìðññáβóá íá áέέÛíáóá áóóò òì ùñéì (÷ ùñβò íá ìáóááèòóóβóáóá ðÛέέ òì ðòñáíá óáo éάέ íá èÛíáóá reboot) ÷ ñçóέììðìέáíóáò όçí sysctl(8) όέìÐ net.inet.ip.fw.verbose\_limit.

2. ÈÛðìéì èÛèò ðñÝðáé íá Ýáέíá. Áέèìýçéóá óέò áíóìéÝò éáoÛ ãñÛíá éάέ όþñá èèáέäþèçéá áðÝñ.

Áóóòò ì ìäçäùò òðìéÝðáé ùóέ ÷ ñçóέììðìέáβóá òì *userland-ppp*, áέ áóóò èέ ìé éáfííáð ðìò áβñíóáé ÷ ñçóέììðìέíýì òì tun0 interface, ðìò áíóέóóìé÷ áβ óόçí ðñþόç όγíááόç ðìò óóέÛ÷ íáóáé ìá òì ppp(8) (áέέέþò áñóóò èάέ ùò *user-ppp*). Ç áðñíáíç όγíááόç éá ÷ ñçóέììðìέíýóá òì tun1, ìáóÛ òì tun2 éάέ ðÛáέ èÝáñíóáò.

Èá ðñÝðáé áðβόçò íá èòìÛóóá ùóέ òì pppd(8) ÷ ñçóέììðìέáβ òì interface ppp0, ìðòá áí ìáέέíáóáóá όç όγíááόÐ óáo ìá òì pppd(8) éá ðñÝðáé íá áíóέéáóáóóðáóá òì tun0 ìá ppp0. ÐáñáέÛóò éá ááβñíóíá Ýíá áýέèì ðñùðì íá áέέÛíáóá òìòò éáfííáð òìò firewall éáoðÛέçéá. Ìé áñ÷έέìβ éáfííáð όþæííóáé 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 éáóáέÛááóá áí ÷ ñçóέììðìέáβóá òì ppp(8) Ð òì pppd(8) ìðññáβóá íá áñáóÛóáóá όçí Ýññáì όçò ifconfig(8) áóìý áñáñáñðìέçéáβ ç όγíááόÐ óáo. Ð.÷., áέá ìéá όγíááόç ðìò áñáñáñðìέçéçéá áðñ òì pppd(8) éá ááβóá èÛóέ óáf áóóò (ááβ÷ñíóáé ìùì ìé ó÷áóέéÝò ãñáñìÝò):

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

Άðñ όçí Ûέçç, áέá ìéá όγíááόç ðìò áñáñáñðìέçéçéá ìá òì ppp(8) (*user-ppp*) èÛ ðñáðá íá ááβóá èÛóέ ðáñññìέì ìá òì ðáñáέÛóò:

```
% 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...)
```