

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.
ÐñēēΥò áðù óéò ēΥìáéò ð õñÛóáéò ïé ïðĩßàò ÷ ñçóéììðñēìγìóáé áðù òĩòò éáóáóéãáóóðΥò ð òĩòò
ðñēçôΥò òĩòò áéá íá áéáéñññĩòĩ óá ðñĩùìíóá òĩòò éãùññĩγìóáé ãìðñééÛ óγìãñē. ¼ðñò áóðΥò
ãìðáíβæìíóáé óá áóðù òĩ éãßìãñ éáé áéá ùóáò áðù áóðΥò ãìùññæáé ç ììÛáá ÁíÛððçĩçò òĩò FreeBSD ùóé
åβιάé ðééáìíí íá áβιάé ãìðñééÛ óγìãñē, éá åãßòá Υία áðù óá óγìãñē: “TM” ð “®”.

Áóðù òĩ Ûñēññ ðãñéãñÛóáé ðñò ìðñãßòá íá ñðēìßóáòá Υία ôåß÷ìò ðñĩóóáóßàò (firewall) ÷ ñçóéììðñēìγìóáò
ìéá PPP óγìãñēç ìΎóù òçäåöþñĩò óôĩ FreeBSD ìá òĩ IPFW. Ðéì óðãéãñēçìΥία, ðãñéãñÛóáé òç ñγέìéóç áñòð
ôåß÷ìò ðñĩóóáóßàò óá ìéá óγìãñēç ìΎóù òçäåöþñĩò ðñò Υ÷áé ãñíãñéç IP áéãýðçĩç. Áóðù òĩ éãßìãñ ããí
áó÷ñéãßóáé ìá òĩ ðñò éá ñðēìßóáòá òçí ãñ÷éç óáò óγìãñēç ìΎóù PPP. Áéá ðãñéóóóðãñãò ðççññññßàò
ó÷ãðééÛ ìá ðéò ñðēìßóáéò ìéáò óγìãñēç ìΎóù PPP åãßòá òç óãñæáá ãñðéãáò ppp(8).

1 Ðññēññò

Áóðù òĩ éãßìãñ ðãñéãñÛóáé òçí áéãáééáóßá ðñò ÷ ñáéÛæáóáé áéá íá ñðēìßóáòá Υία ôåß÷ìò ðñĩóóáóßàò óôĩ
FreeBSD ùóáí ç IP áéãýðçĩç ãßíáóáé ãñíãñééÛ áðù òĩ ISP óáò. Ðãñññē ðñò Υ÷ù ðñĩóðáéðóáé íá ēÛñ áóðù òĩ
éãßìãñ ùóí òĩ ãñíãññ ðéì ðçðñãò éáé óùóðù, åãßòá ãððññóáãðñé íá óðãñæáòá ðéò áéññèðóáéò, óá ó÷ñééá ð ðéò
ðññòÛóáéò óáò óðç áéãýðçĩç òñò óðããñãóΥά: <marcs@draenor.org>.

2 ÐãñÛìáðññé òñò ððññía

Áéá íá ìðñΥóáòá íá ÷ ñçóéììðñēìγìóáòá òĩ IPFW, ðñΥðáé íá áíóùìáððóáòá òçí ó÷ãðééç ððñññññçç óôñ ððññía óáò.
Áéá ðãñéóóóðãñãò ðççññññßàò ó÷ãðééÛ ìá òç ìáðáãèððéóç òñò ððññía, åãßòá òĩ òññía ñðēìßóáñ òñò ððññía óôñ
Ãã÷áéñßáéñ (http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html). Éá ðñΥðáé íá
ðññéçΥóáòá ðéò ðãñáéÛò ãðçññΥò óðéò ñðēìßóáéò òñò ððññía óáò áéá íá áñãñãñðñéçðóáòá òçí ððñññññçç áéá òĩ
IPFW:

```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεέα οᾶβ÷ἰοο δñιόοάοβào οἰῶ δῶñΠία.

ΌγιαΒυός: Άδου οι έαβιαί έαυηάβ υός Ύ÷ άόά άάέάόάόΠόάέ όγι Ύέαιός 5.X οιό FreeBSD Π ιέα όεί όηύόόάό. Αί ÷ήόόείόίείάβόά όγι Ύέαιός 4.X, όύόά έά όηΎόάέ ίά άίάηάίόίέΠόάόά όγι άόέείαΠ *IPFW2* έάέ ίά άέάάΎόάόά ός όάέβάά άίΠεάέό ipfw(8) έέά όηέόόόύόόηάό όέόηίόίηβάό ό÷ άόέέΎ ίά όγι άόέείαΠ *IPFW2*. ΠηίόΎίόά έάέάβόάηά όί 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
```

Ἄϋααε εὐϋιεῖ ὑνεῖ ὁδεὸ ὠνῆδ ὁῖο εὐϋιεῖα ἀαῆαῶρ εἰ εἰαῶαῆνϋῶαῶε. ὃδε ἰῇηἶβῶα ἰἷ εἰαῶαῆνϋῶαῶα ὁἷ ἰϋῖῖἷἷἷἷ ἅδῦ ὁῖ ὁἶβ÷ῖδ ὅηῖῖῖῖῖῖῖῖῖ ÷ῖηῖδ ὁῖῖ εἶβἷἷῖῖ ἰἷ ἶἷἷῖῖῖῖ ὁἷ ἶἷ ÷ ἶβἷ εἰαῶαῆἷἷῖῖῖ ὁῖο ὁῖῖῖῖῖῖῖῖ ὁἷ ἶἷ ἶἷ ÷ ἶἷῖῖῖῖ εὐϋιεῖα ἶῖῖῖῖῖ. Ὅῖ ὑνεῖ 500 ἰϋῖῖῖῖῖῖ ἶἷἷἷ ἰἷἷ ἶἷῖῖῖῖ ἷἷῖῖῖῖ ὁῖῖ, ἶῖῖῖ ἰῇηἷἷῖῖῖ ἰἷ ὅηῖῖῖῖῖῖῖῖῖ ἶῖῖῖ ὁῖῖ ὁῖῖ ἶῖῖῖῖῖ ἶῖῖῖῖῖ ἶῖ ὁῖῖ ἶῖῖῖῖῖ ἶῖ ὁῖῖ ἶῖῖῖῖῖῖῖ ὁῖο ἶῖῖῖῖ ὁἷ ἶῖῖῖῖῖῖῖῖ.

```
options IPDIVER
```

Āīāñāīōīēāβ ōā *divert* sockets, ðīō èā āīyīā āñāūōāñā ōē ēŪīīōī.

[illegible]

3 ÁëéãÑò óôi /etc/rc.conf ãéá íá öĩñôþíáôáé ôĩ ôâß÷ìò
ðñĩóôáóßáò

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

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

Άέά έάνέόόώδάνάό δέçñröivñßáó ó-άόέéŨ íà όç όçíáoßáó éáέáíéŨó áðü áòóŸó óέó άάáiŸó, ñßíôá íéá íáόéŨ óóí /etc/default/rc.conf éάé áéááŨóóá όçí man óάßáá rc.conf(5)

4 ΆíññìðìεΠόοά όçí ΑίούìάòùìΎίç ìάòÛñάόç Äέάðέγíόάùì όìò PPP

Άέά íá äðέòñÝðáòά óá Ûέέά ìç÷áíΠíάóá όìò äέέóγíò óáò íá óóíáΎííóáέ ìά όìí Ύíù έùóìí ìΎóù όìò FreeBSD, ÷ñçóέìíðìεΠíόáò όì ùò “ðýέç”, έá ðñÝðáέ íá áíñññìðìεΠόóáò όçí ΑίούìάòùìΎίç ìάòÛñάόç äέάðέγíόáùì όìò PPP (NAT). Άέά íá áβíáέ áòòù, ðñìóεΎóóá óòì áñ÷áβì /etc/rc.conf óέò ðáñáέÛòù áñáñΎò:

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

Όόç εΎόç όìò ðñìòβέ_ðçò_όγíääóçò ðñÝðáέ íá áÛέáòά όì ùíñά óçò óγíääóçò óáò, ùòòù όì Ύ÷áòά áðìεçέáγóáέ óòì áñ÷áβì /etc/ppp/ppp.conf.

5 Ìέ έáíüíáò όìò firewall

Όì ùíñ όìò áðñΎíáέ όðñά áβíáέ íá ìñβóìòìά όìòð έáíüíáò όìò firewall. Ìέ έáíüíáò όìòð ìðìβìòð ðáñέáñÛóìòìά ááð áβíáέ áñέáòÛ έáέìβ áέá όìòð ðáñέóóùòáñìòð ÷ñΠόóáò ìά dialup óγíääóç, áέέÛ ìγóά óðì÷ñáùóέέìβ áβíáέ, ìγóά áβíáέ áóíáòùì íá óáέñέÛέìòì ìά óέò áíÛáέáò ùέùì óùì ÷ñçóóðí dialup. Ìðìñíγí, ùìòð, íá ÷ñçóέìáγóìòì ùò Ύíá έáέù ðáñÛáέέìá ñòέìβóáùì όìò IPFW έáέ áβíáέ ó÷áðέέÛ áγέìèí íá όìòð ðñìóáñìüóáòά óóέò äέέΎò óáò áíÛáέáò.

Áò áñ÷áβóìòìά ùìòð ìά óέò ááóέέΎò áñ÷Ύò áíüò έέáέóóíγ óáβ÷ìòð ðñìóóáóáò. Íá έέáέóóù óáβ÷ìòð ðñìóóáóáò áðááññáγáέ έáò’ áñ÷Πí έÛέá óγíääóç. Ì áέá÷áέñέóóðð ìðìñáβ γóóáñά íá ðñìóεΎóáέ έáíüíáò áέá íá äðέòñÝðáέ ìüíí óóáέáñέñéΎíáò óóíáΎóáέò íá ðáñíÛíá áðù όì óáβ÷ìòð ðñìóóáóáò. Ç ðéì óðìçέέóìΎίç óáέñÛ óùì έáíüíüí óá Ύíá έέáέóóù óáβ÷ìòð áβíáέ: ðñðóά ìέ έáíüíáò όìò äðέòñÝðìòì ìáñέέΎò óóíáΎóáέò, έáέ óΎέìò ìέ έáíüíáò όìò áðááññáγíòì ìðìέááΠðìòά Ûέέç óγíääóç. Ç εíáέέΠ ðβóù áðù áòòù áβíáέ ùóέ ðñðóά áÛάóáò όìòð έáíüíáò όìò äðέòñÝðìòì ðñÛáíáóά íá ðáñÛóìòì έáέ γóóáñά ùέá óá Ûέέá áðááññáγííóáέ áòòùìáóά.

ΌðέÛìòά, εíέðùí, Ύíá έáòÛέìáí óóìí ìðìβì έá áðìεçέáγííóáέ ìέ έáíüíáò όìò óáβ÷ìòð ðñìóóáóáò. Όά áòòù όì Ûñέñí ÷ñçóέìíðìεíγíá ùò ðáñÛáέέìá όìí έáòÛέìáí /etc/firewall. ΆέέÛìòά έáòÛέìáí ìΎóá óá áòòùí έáέ äçìέìòñáΠóóá όì áñ÷áβì fwrules όìò όì ùíñÛ όìò áβ÷áíá áñÛáέ óòì rc.conf. ΌçìáέΠóóá ðùò ìðìñáβóά íá áέέÛíáòά όì ùíñά όìò áñ÷áβìò áòòíγ óá ùóέ εΎέáòά. Áòòùò ì ìαçäùò áβíáέ áòòù όì ùíñά óáí ðáñÛáέέìá έáέ ìüíí.

Áò äíγíá όðñά Ύíá ðáñÛáέέìá óáβ÷ìòð ðñìóóáóáò ìά áñέáòÛ áðáíçäçíáðέέÛ ó÷úέέá.

```
# 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
```

Όπná Ý÷áoá Ýía ðēēçñüíÝíí óåβ÷ìò ðñüóóáóβáo, òì ïðßì óóíaÝóáéo óóéo èýñáo 22 éáé 80 éáé éáoáñÜöáé üēáo óéo Üēēáo óóíaÝóáéo óôi áñ÷åßì éáoáñáoðò òìò óóóðßáoìò. ÐēÝíí åβóðå Ýðēñē áéá åðáíæēßçóc. Ôì óåβ÷ìò ðñüóóáóβáo éå áíåññðēçēåß áóðüíáoá éáé éå òñòðóå òìò éáíüáo ðìò ðñüóēÝóáoå. Áí åå åßíæé áóðü Þ Ý÷áoå ïðēååððìòå ðñüæßáoå, Þ áí Ý÷áoå èÜðēáo ðñüÜóáéo áéá íå áéññēèååß áóðü òì Üñēñì, åðēñēñüíßóóå íææ ïìò íå email.

6 ÅñüòÞóáéo

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

Áóðü áðēÜ óçíåíåé ðüò Ý÷å ðñóέññðēçēåß òì ïÝáέóôi ùñēñ éáoáñáoðò (logging) áéá áóðü òì éáíüå. Ì éáíüå ï ßæìò áíæññðēåß íå æñçåýåé, áéèÜ ååñ éå óóÝñíæé ðéå ìçíýíáoå óôi áñ÷åßì éáoáñáoðò òìò óóóðßáoìò ïÝ÷ñé íå ìçåñíóóåðð èÜçé òìò ìåñçóÝò. Ìðñåßóå íå ìçåñíóóåðð òìò ìåñçóÝò ìå ççí áññēÞ

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáßóá íá áðìßóáóá òì ùñέì éάόάññáößò óóέò ñòèìßóáέò òìò ðòñßíá óάò ìá όçí áðέέìāß IPFWALL_VERBOSE_LIMIT ùðòò ðññέññÛðáìá ðññáðÛì. ìðññáßóá íá áέέÛíáóá áóòò òì ùñέì (÷ ùñßò íá ìáóáäèùóóßóáóá ðÛέέ òì ðòñßíá óάò éάέ íá èÛíáóá reboot) ÷ ñçóέììðìέßíóáò όçí sysctl(8) όέìß net.inet.ip.fw.verbose_limit.

2. ÈÛðìέì èÛèò ðñÝðáέ íá Ýáέíá. Áέèìέçóá óέò áíòìέÝò éάóÛ ãñÛìá éάέ όþñá èèáέäþèçéá áðÝì.

Áóòòò ì ìäçäùò òðìέÝðáέ ùóέ ÷ ñçóέììðìέáßóá òì *userland-ppp*, äé áóòò èέ ìé éáfííáð ðìò äßñíóáέ ÷ ñçóέììðìέíýì òì tun0 interface, ðìò áíóέóòìέ÷ áß óόçì ðñþόç óýíááόç ðìò óóέÛ÷ íáóáέ ìá òì ppp(8) (áέέέþò áñóòò éάέ ùò *user-ppp*). Ç áðñíáíç óýíááόç éá ÷ ñçóέììðìέíýóá òì tun1, ìáóÛ òì tun2 éάέ ðÛáέ èÝññíóáò.

Èá ðñÝðáέ áðßόçò íá èòìÛóóá ùóέ òì pppd(8) ÷ ñçóέììðìέáß òì interface ppp0, ìðòá áí ìáέέìßóáóá όç óýíááόß óάò ìá òì pppd(8) éá ðñÝðáέ íá áíóέéάóáóóßóáóá òì tun0 ìá ppp0. ÐññáέÛòù éá äáßñíòìá Ýíá áýέìέì ðññðì íá áέέÛíáóá òìòò éáfííáð òìò firewall éάóÛέέçéá. ìé ãñ÷έέìß éáfííáð όþñííóáέ óá Ýíá ãñ÷áßì 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 éάóáέÛááóá áí ÷ ñçóέììðìέáßóá òì ppp(8) ð òì pppd(8) ìðññáßóá íá áíáóÛóáóá όçì Ýñññì όçò ifconfig(8) áóìý áíáñññðìέçéáß ç óýíááόß óάò. Ð.÷., äéá ìéá óýíááόç ðìò áíáñññðìέçéçéá áðù òì pppd(8) éá äáßóá èÛóέ óáf áóòò (äáß÷ñíóáέ ìñì ìé ó÷áóέέÝò ãñññìÝò):

```
% 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 Ûέέç, äéá ìéá óýíááόç ðìò áíáñññðìέçéçéá ìá òì ppp(8) (*user-ppp*) èÛ ðññðá íá äáßóá èÛóέ ðññññέì ìá òì ðññáέÛòù:

```
% 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...)
```