

Όγιάαός ΙΎού Όçäåöþĩõ éáé Ôåß÷ìò Ðñĩóôáóßàò óôĩ FreeBSD

Marc Silver

marcs@draenor.org

\$FreeBSD: release/9.1.0/el_GR.ISO8859-7/articles/dialup-firewall/article.shtml
38826 2012-05-17 19:12:14Z hrs \$

Ôĩ FreeBSD áβιάέ Υία éáôĩ÷ðñũĩΥĩĩ àìðĩñéêũ óγĩáĩēĩ òĩõ FreeBSD Foundation.
ÐĩēēΥò áðũ óéò ēΥĩáéò Þ òñŬóáéò íē ïðĩßàò ÷ ñçóéĩðĩēĩγĩóáé áðũ òĩõò éáóáóēáóáóôΥò Þ òĩõò
ðũēçôΥò òĩõò áéá íá áéáēñβĩĩôĩ óá ðñĩũĩóá òĩõò éåũñĩγĩóáé àìðĩñéêũ óγĩáĩēá. ¼ðĩõ áóôΥò
àìðáĩβēĩĩóáé óá áóôũ òĩ éåβĩáĩĩ éáé áéá ũóáò áðũ áóôΥò àĩũñβæáé ç ìŬáá ÁĩŬðòðĩçò òĩõ FreeBSD ũóé
åβιάέ ðééáĩũĩ íá áβιάέ àìðĩñéêũ óγĩáĩēá, éá ååßðá Υία áðũ óá óγĩáĩēá: “TM” Þ “©”.

Áóôũ òĩ Ŭñēñĩ ðåñéåñŬóáé ðũð ìðñåßðá íá ñðēĩßóáðá Υία ôåß÷ìò ðñĩóóáóßàò (firewall) ÷ ñçóéĩðĩēĩγĩóáò
íéá PPP óγĩááóç ìΎού όçäåöþĩõ óôĩ FreeBSD ìå òĩ IPFW. Ðēĩ óðæåēñēĩΥĩá, ðåñéåñŬóáé όç ñγēĩéόç áĩũð
ôåß÷ìò ðñĩóóáóßàò óá íéá óγĩááóç ìΎού όçäåöþĩõ ðĩõ Υ÷å áóĩáĩéêÞ IP áéåγēðĩόç. Áóôũ òĩ éåβĩáĩĩ åáĩ
áó÷ìååßðáé ìå òĩ ðũð éå ñðēĩßóáðá όçĩ åñ÷éêÞ óáð óγĩááóç ìΎού PPP. Áéá ðåñéóóũðåñåð ðēçñĩõñβåð
ó÷åðéēŬ ìå óéð ñðēĩßóáéò íéáð óγĩááóç ìΎού PPP ååßðá όç óåēßåå åĩÞéåáð ppp(8).

1 Ðñũēĩāĩò

Áóôũ òĩ éåβĩáĩĩ ðåñéåñŬóáé όçĩ áéååééåóßá ðĩõ ÷ ñåéŬæåðáé áéá íá ñðēĩßóáðá Υία ôåß÷ìò ðñĩóóáóßàò óôĩ
FreeBSD ũóáĩ ç IP áéåγēðĩόç åβĩáðáé áóĩáĩéēŬ áðũ òĩĩ ISP óáð. Ðåñũēĩ ðĩõ Υ÷ũ ðñĩóðåêÞóáé íá ēŬũ áóôũ òĩ
éåβĩáĩĩ ũóĩ òĩ áóĩáóũĩ ðēĩ ðēÞñåð éáé óũóðũ, åßóðå áððñũóååðéé íá óðåßåðå ðéð áéĩñēÞóáéð, óá ó÷ũééá Þ óéð
ðñĩóŬóáéð óáð óόç áéåγēðĩόç òĩõ óðååñåðŬá: <marcs@draenor.org>.

2 ÐåñŬĩåðñĩé òĩõ ððñÞĩá

Áéá íá ìðñŬóáðá íá ÷ ñçóéĩðĩēĩÞóáðá òĩ IPFW, ðñŬðåé íá áĩóũĩåðÞóáðá όçĩ ó÷åðéêÞ ððĩóðÞñēĩç óôĩĩ ððñÞĩá óáð.
Áéá ðåñéóóũðåñåð ðēçñĩõñβåð ó÷åðéēŬ ìå όç ìåðååÞððéόç òĩõ ððñÞĩá, ååßðå òĩ òĩÞĩá ñðēĩßóáũĩ òĩõ ððñÞĩá óôĩ
Åå÷åñβāēĩ (http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html). Éå ðñŬðåé íá
ðñĩóēΥóáðå óéð ðåñåēŬðũ åðēĩāŬò óðéð ñðēĩßóáéð òĩõ ððñÞĩá óáð áéá íá áĩåñāĩðĩēĩÞóáðå όçĩ ððĩóðÞñēĩç áéá òĩ
IPFW:

```
options IPFWALL
```

Αἰᾶναιδιεᾶβ οἱί ἐπαεεᾶ οᾶβ÷ἰοο δñιόοᾶόβαο οἰῶ δῶñΠία.

ΌγίαΒυός: Άόου οί έαβιαί έαυηάβ υόε Ύ÷ άόά άάέάόάόΠόάέ όγί Ύέαιός 5.X οίθ FreeBSD Π ιέα όεί όηύόόάό. Αί ÷ήόόείήίέαβόά όγί Ύέαιός 4.X, όυόά έά όηΎόάέ ίά άίάηάήίέΠόάόά όγί άόέέϊΑΠ *IPFW2* έάέ ίά άέάάΎόάόά ός όάέβάά άίΠεάέό ipfw(8) έέά όηέόόόύόόηάό όέόηίόήηβάό ό÷ άόέέΎ ίά όγί άόέέϊΑΠ *IPFW2*. ΠήιόΎίόά έάέάβόάηά όί όίΠιά *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFWALL VERBOSE
```

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

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

[illegible]

```
options IPDIVER
```

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

[illegible]

3 ÁëëãÑò 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 óäëBää rc.conf(5)

4 ΆíññìðìέΠóòά όçí ΑίóύìáòùìΎίç ìáòÛññάόç Äέáðēýíóáùì óìò PPP

Άέά íá äðέòñÝðáòά óá Ûέέá ìç÷áíΠíáòά òìò äέέóýìò óáò íá óòíáΎìíóáέ ìá òìí Ύìù èùòìí ìΎóù òìò FreeBSD, ÷ñçóέììðìέΠíóáò òì ùò “ðýέç”, έá ðñÝðáέ íá áíñññìðìέΠóòάά όçí ΑίóύìáòùìΎίç ìáòÛññάόç äέáðēýíóáùì òìò PPP (NAT). Άέά íá áβíáέ áòòù, ðñìóέΎóáά óòì áñ÷áβì /etc/rc.conf óέò ðáñáέÛòù áñáñìΎò:

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

Όόç èΎόç òìò ðñìòβέ_όçò_όγíääóçò ðñÝðáέ íá áÛέáòά òì ùíñá όçò óγíääóçò óáò, ùòòù òì Ύ÷áòά áðìέçέáýóáέ óòì áñ÷áβì /etc/ppp/ppp.conf.

5 Ìέ έáíüíáò òìò firewall

Όì ìüñ ðìò áðñΎíáέ òðñά áβíáέ íá ìñβóìòìá òìò έáíüíáò òìò firewall. Ìέ έáíüíáò òìò ìðìβìòð ðáñέáñÛòìòìá ááð áβíáέ áñέáòÛ έáέìβ áέá òìòð ðáñέóóùòáñìòð ÷ñΠóóáò ìá dialup óγíääóç, áέέÛ ìýóá òðì÷ñáùóέέìβ áβíáέ, ìýóá áβíáέ áòíáòùì íá óáέñέÛέìòì íá óέò áíÛáέò ùέùì òùì ÷ñçóòðí dialup. Ìðìñìýí, ùìò, íá ÷ñçóέìáýóìòì ùò Ύíá έáέù ðáñÛáέέìá ñòèìβóáùì òìò IPFW έάέ áβíáέ ó÷áòέέÛ áýέìèí íá òìòð ðñìóáñìüóáòά óóέò áέέΎò óáò áíÛáέò.

Áò áñ÷áβìòìá ùìò ìá óέò ááóέέΎò áñ÷Ύò áíüò èέáέóòìý óáβ÷ìòð ðñìóóáóáò. Íá èέáέóòù óáβ÷ìò ðñìóóáóáò áðááññáýáέ έáò’ áñ÷Πí έÛέá óγíääóç. Ì áέá÷áέñέóóð ìðìñáβ ýóóáñά íá ðñìóέΎóáέ έáíüíáò áέá íá äðέòñÝðáέ ìüñ óóáέáèñέíΎíáò óòíáΎóáέò íá ðáñìÛíá áðù òì óáβ÷ìò ðñìóóáóáò. Ç ðέì óòìçέέòìΎίç óáέñÛ òùì έáíüíüí óá Ύíá èέáέóòù óáβ÷ìò áβíáέ: ðñðóá ìέ έáíüíáò ðìò äðέòñÝðìòì ìáñέέΎò óòíáΎóáέò, έάέ òΎέìò ìέ έáíüíáò ðìò áðááññáýìòì ìðìέááΠðìòά Ûέέç óγíääóç. Ç έìáέέΠ ðβóù áðù áòòù áβíáέ ùóέ ðñðóá áÛέáòά òìòð έáíüíáò ðìò äðέòñÝðìòì ðñÛáíáòά íá ðáñÛóìòì έάέ ýóóáñά ùέá óá Ûέέá áðááññáýìíóáέ áòòùìáóά.

ΌóέÛìòά, έìέðùì, Ύíá έáòÛέìáí óòìí ìðìβì έá áðìέçέáýìíóáέ ìέ έáíüíáò òìò óáβ÷ìòð ðñìóóáóáò. Όά áòòù òì Ûñèññ ÷ñçóέììðìέíýíá ùò ðáñÛáέέìá òìí έáòÛέìáí /etc/firewall. ΆέέÛìòά έáòÛέìáí ìΎóá óá áòòùì έάέ äçìέìòñáΠóóά òì áñ÷áβì fwrules ðìò òì ùíñÛ òìò áβ÷áíá áñÛóáέ óòì rc.conf. ΌçìáέΠóóά ðùò ìðìñáβóá íá áέέÛìáòά òì ùíñá òìò áñ÷áβìò áòòìý óá ùóέ èΎέáòά. Áòòùò ì ìäçäùò áβíáέ áòòù òì ùíñá óáí ðáñÛáέέìá έάέ ìüñ.

Áò äìýíá òðñά Ύíá ðáñÛáέέìá óáβ÷ìòð ðñìóóáóáò ìá áñέáòÛ áðáíçäçìáóέέÛ 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 óðiaÝóáéoð óôi áñ÷åβì éáoáñáoðò òìò óóóðìáoòìò. ÐēÝíí åβóðå Ýðìēñē áéá åðáíæēβìçóc. Ôì óåβ÷ìò ðñüóóáóβáo éå áíåññðìēçēåβ áóðüíáoá éáé éå òñòðóáé òìòð éáíüíáo ðìò ðñìóēÝóáoå. Áí åå åβíáé áóðü ð Ý÷áoå ððìéååððìóå ðñìæðìáoå, ð áí Ý÷áoå èÜðìéáo ðñìóÜóáéoð áéá íå áéññēùēåβ áóðü òì Üñēñì, åðéēñēñìðóóå íææβ ììò íå email.

6 Åñùòðóáéoò

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

Áóðü áðēÜ óçíåβíåé ðüò Ý÷åé ðñóéñìðìēçēåβ òì ìÝáéóòì üñēñ éáoáñáoðò (logging) áéá áóðü òì éáíüíå. Ì éáíüíå ì βæìò áíæññòēåβ íå æìçåýåé, áēēÜ ååñ éå óóÝñíåé ðéå ìçíýíáoå óôi áñ÷åβì éáoáñáoðò òìò óóóðìáoòìò ìÝ÷ñé íå ìçåñíóáoå ðÜēé òìò ìåññçóÝò. Ìðñåβóå íå ìçåñíóáoå òìò ìåññçóÝò ìå òçííñìð

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáßóá íá áðìßóáóá òì ùñέì éάόάññáößò óóέò ñòèìßóáέò òìò ðòñßíá óáo ìá όçí áðέέìāß IPFWALL_VERBOSE_LIMIT ùðòò ðññέññÛðáì ðññáðÛì. ìðññáßóá íá áέέÛíáóá áóóò òì ùñέì (÷ ùñßò íá ìáóáæèòóóßóáá ðÛέέ òì ðòñßíá óáo éάέ íá èÛíáóá reboot) ÷ ñçóέììðìέßíóáó όçí sysctl(8) όέìß net.inet.ip.fw.verbose_limit.

2. ÈÛðìέì èÛèò ðñÝðáέ íá Ýáέíá. Áέèìέçóá óέò áíòìέÝò éáoÛ ãñÛìá éάέ όþñá èèáέäþέçéá áðÝì.

Áóóòò ì ìäçäùò òðìέÝðáέ ùóέ ÷ ñçóέììðìέáßóá òì *userland-ppp*, áέ áóóò èέ ìέ éáfííáð ðìò äßñíóáέ ÷ ñçóέììðìέíýì òì tun0 interface, ðìò áíóέóóìέ÷ äß óόçì ðñþόç óýíááόç ðìò óóέÛ÷ íáóáέ ìá òì ppp(8) (áέέέþò áñóóò èάέ ùò *user-ppp*). Ç áðñíáíç óýíááόç éá ÷ ñçóέììðìέíýóá òì tun1, ìáóÛ òì tun2 éάέ ðÛáέ èÝáñíóáó.

Èá ðñÝðáέ áðßόçò íá èòìÛóóá ùóέ òì pppd(8) ÷ ñçóέììðìέáß òì interface ppp0, ìðòá áí ìáέέìßóáóá όç óýíááόß óáo ìá òì pppd(8) éá ðñÝðáέ íá áíóέéάóáóóßóáá òì tun0 ìá ppp0. ÐññáέÛóò éá ääßñíóìá Ýíá áýέìέì ðññðì íá áέέÛíáóá òìòò éáfííáð òìò firewall éáoðÛέέçéá. ìέ äñ÷έέìß éáfííáð όþæìíóáέ óá Ýíá äñ÷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 áñáóÛóáóá όçì Ýññì όçò ifconfig(8) áóìý áññññðìέçéäß ç óýíááόß óáo. Ð.÷., áέá ìέá óýíááόç ðìò áññññðìέçéçéá áðñ òì pppd(8) éá ääßóá èÛóέ óáf áóóò (ääß÷ñíóáέ ìñì ìέ ó÷äóέέÝò ãñññÝò):

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

Άðñ όçì Ûέέç, áέá ìέá óýíááόç ðìò áññññðìέçéçéá ìá òì ppp(8) (*user-ppp*) èÛ ðññðá íá ääßóá èÛóέ ðññññέì ìá òì ðññáέÛóò:

```
% 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...)
```