

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 ÷ ñçóéìĩðñēĩγìóáé áðù ôĩõò éáóáóéäåóáóðΥò ð ôĩõò
ðñēçðΥò ôĩõò áéá íá äéáēñßñĩôĩ óá ðñĩùũíóá ôĩõò èàùññĩγìóáé àìðñééÛ óγìáĩēá. ¼ðñĩ áóðΥò
àìðáíßæñĩóáé óá áðù òĩ èáßìáñĩ éáé áéá ùóáò 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 ðùò ïðñāßðá íá ñðēĩßóáðá Υία ôåß÷ĩò ðñĩóðáóßàò (firewall) ÷ ñçóéìĩðñēĩγìóáò
ìéá PPP óγìááóç ìΎúò òçäåöþñĩõ óôĩ FreeBSD ìá ôĩ IPFW. Ðéĩ óðäēäēñēĩΥία, ðñéñāñÛóáé òç ñγέìéóç áñùð
ôåß÷ĩò ðñĩóðáóßàò óá ìéá óγìááóç ìΎúò òçäåöþñĩõ ðñĩ Õ÷áé äñíáíēēð IP äéäγέðñĩõ. Áðù òĩ èáßìáñĩ äáí
áó÷ñēåßðáé ìá ôĩ ðùò éá ñðēĩßóáðá òçí áñ÷éēð óáð óγìááóç ìΎúò PPP. Áéá ðñéóóóðñāñð ðççññĩõñßàò
ó÷áðéēÛ ìá ðéò ñðēĩßóáðéò ìéáð óγìááóç ìΎúò PPP åáßðá òç óåßßáá àñðéäéáð ppp(8).

1 Ðññēĩñĩò

Áðù òĩ èáßìáñĩ ðñéñāñÛóáé òçí äéäéééáóßá ðñĩ ÷ñāéÛæåóáé áéá íá ñðēĩßóáðá Υία ôåß÷ĩò ðñĩóðáóßàò óôĩ
FreeBSD ùðáí ç IP äéäγέðñĩõ äßñáðáé äñíáíēēÛ áðù òĩ ISP óáð. Ðáñññēĩ ðñĩ Õ÷÷ ðñĩóðáéðóáé íá èÛñ áðù òĩ
èáßìáñĩ ùóĩ òĩ äñíáðñĩ ðéĩ ðēðñāð éáé óùóðù, åáßðá äððññóáäðñē íá óðåßäðá ðéò äéññēðóáðéò, óá ó÷ñēéá ð ðéò
ðññòÛóáðéò óáð óðç äéäγέðñĩõ òñĩ óðāññāóΥá: <marcs@draenor.org>.

2 ÐáñÛìáðññē ôĩõ ððññía

Áéá íá ìðñΥóáðá íá ÷ ñçóéìĩðñēĩγìóáðá ôĩ IPFW, ðñΥðáé íá áíóùìáððóáðá òçí ó÷áðéēð ððñóðññēĩç óôĩ ððññía óáð.
Áéá ðñéóóóðñāñð ðççññĩõñßàò ó÷áðéēÛ ìá òç ìáðāæðððéóç òñĩ ððññía, åáßðá ôĩ òññía ñðēĩßóáñĩ òñĩ ððññía óôĩ
Åā÷áññßäēĩ (http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html). Éá ðñΥðáé íá
ðññéΥóáðá ðéò ðñāñéÛðù äðéēñāΥð óðéò ñðēĩßóáðéò òñĩ ððññía óáð áéá íá áññāñññēĩγìóáðá òçí ððñóðññēĩç áéá ôĩ
IPFW:

```
options IPFW2
```

Άίᾱñᾱῖðῖḗâß òîῖ ḗþᾱḗḗ ḡâß÷ìðð Ññíóðáóßáð òîð ððñÞᾱ.

Ὀçἰᾱßùç: Ἀðð òῖ ḗâßᾱῖῖ ḗâùñᾱß ùðḗ Ḣ÷ᾱðᾱ ᾱᾱḗᾱðáððÞᾱḗ ḡçἰ Ḣḗᾱῖç 5.X òîð FreeBSD Þ ἱḗᾱ ḡḗῖ ðñùððáðç. Ἀἰ ðñçóḗἰðῖḗâßðᾱ ḡçἰ Ḣḗᾱῖç 4.X, ðùðᾱ ḗᾱ ðñÝðᾱḗ ἱᾱ ᾱἰᾱñᾱῖðῖḗÞᾱðᾱ ḡçἰ ᾱðḗḗᾱÞ IPFW2 ἑᾱḗ ἱᾱ ᾱḗᾱᾱÛððᾱ ḡç ḡᾱḗßᾱᾱ ᾱῖÞḗᾱḗᾱð ipfw(8) ᾱḗᾱ ðᾱñḗóóùðᾱñᾱð ðḗçñἰðἰñßᾱð ó÷ᾱðḗḗÛ ἱᾱ ḡçἰ ᾱðḗḗᾱÞ IPFW2. ðñἰóÝἰðᾱ ḗᾱḗᾱßðᾱñᾱ òῖ ðἰÞᾱ USING IPFW2 IN FreeBSD-STABLE.

```
options IPFW2_VERBOSE
```

ὈðÝḗᾱḗ ḡᾱ ἱçἰἱᾱðᾱ ᾱḗᾱ ḡᾱ ḗᾱðÛḗḗçḗᾱ ḡᾱḗÝḡᾱ ḡἰῖ log òîð ḡðððÞᾱðἰð.

```
options IPFW2_VERBOSE_LIMIT=500
```

ἈÛᾱḗ ḗÛðῖḗῖ ṽñḗῖ ḡðḗð ṽñÝð ðἰð ḗÛðῖᾱ ᾱᾱñᾱðÞ ḗᾱ ḗᾱðᾱñÛðᾱḗ. ḡóḗ ἰðñᾱßðᾱ ἱᾱ ḗᾱðᾱñÛðᾱðᾱ ḡᾱ ἱçἰἱᾱðᾱ ᾱðù ḡῖ ḡâß÷ìðð Ññíóðáóßáð ðññßð ḡἰῖ ḗßἱᾱðἰῖ ἱᾱ ᾱᾱἰßἰἰῖ ḡᾱ ᾱñ÷ᾱßᾱ ḗᾱðᾱñᾱðÞð ḡἰð ḡðððÞᾱðἰð ḡᾱð ᾱἰ ᾱᾱ÷ᾱßðᾱ ḗÛðῖᾱ ᾱðßḗᾱç. Ὀῖ ṽñḗῖ 500 ἱçἰἰÛðἰ ᾱßἱᾱḗ ἱḗᾱ ᾱñḗᾱðÛ ḗῖᾱḗḗÞ ḡḗἰÞ, ᾱḗḗÛ ἰðñᾱßðᾱ ἱᾱ ðñἰóᾱñἰùðᾱðᾱ ᾱððÞ ḡçἰ ḡḗἰÞ ᾱῖÛḗᾱᾱ ἱᾱ ḡḗð ᾱðᾱḗðÞᾱḗð ḡἰð ᾱḗḗἱÝ ḡᾱð ᾱḗḗðÝἰð.

```
options IPDIVERT
```

Άἰᾱñᾱῖðῖḗâß ḡᾱ *divert* sockets, ðἰð ḗᾱ ᾱῖÝἱᾱ ᾱñᾱùðᾱñᾱ ḡḗ ḗÛἰἰῖ.

ðñἰḗḗἰðἰßçç: ἰḗḗḗð ḡᾱḗᾱḗÞᾱðᾱ ἱᾱ ḡḗð ñðḗἰßðᾱḗð ḗᾱḗ ḡçἰ ἱᾱðᾱᾱḗÞððḗçç ḡἰð ððñÞᾱ ḡᾱð ἱçἰ ḗÛἰᾱðᾱ ᾱðᾱἰḗḗßçç! Ἀἰ ḗÛἰᾱðᾱ ᾱðᾱἰḗḗßçç ḡᾱ ᾱððù ḡῖ ḡçἰᾱßἰ ἰðἰñᾱß ἱᾱ ḗḗᾱḗᾱùḗᾱßðᾱ ᾱðÝἰù ᾱðù ḡῖ ḡýðçἰÛ ḡᾱð. ðñÝðᾱḗ ἱᾱ ðᾱñḗἰÝἰᾱðᾱ ἰÝ÷ñḗ ἱᾱ ᾱᾱḗᾱðáððᾱḗἱÝἰ ἱḗ ḗᾱἰἱᾱð ḡἰð ḡâß÷ìðð Ññíóðáóßáð ḗᾱḗ ἱᾱ ᾱἰçἰᾱñἰḗἱÝἰ ṽḗᾱ ḡᾱ ḡ÷ᾱðḗḗÛ ᾱñ÷ᾱßᾱ ñðḗἰßðᾱḷἰ.

3 ἈḗḗᾱᾱÝð ḡἰῖ /etc/rc.conf ᾱḗᾱ ἱᾱ ḡἰñḡÞᾱðᾱḗ ḡῖ ḡâß÷ìð ðñἰóðáóßáð

Ἀḗᾱ ἱᾱ ᾱἰᾱñᾱῖðῖḗâßðᾱḗ ḡῖ ḡâß÷ìðð Ññíóðáóßáð ḗᾱðÛ ḡçἰ ᾱḗḗßççç ḡἰð ḡðððÞᾱðἰð ḗᾱḗ ᾱḗᾱ ἱᾱ ἰñßðᾱðᾱ ḡῖ ᾱñ÷ᾱßἰ ἱᾱ ḡἰðð ḗᾱἱἱᾱð ḡἰð ḡâß÷ìðð ðñἰóðáóßáð, ðñÝðᾱḗ ἱᾱ ᾱἰçἰᾱñÞᾱðᾱ ḡῖ ᾱñ÷ᾱßἰ /etc/rc.conf. ἈðḗÛ ðñἰḗḗÝḡḡᾱ ḡḗð ðᾱñᾱḗÛðù ᾱñᾱἰÝð:

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

Ἀḗᾱ ðᾱñḗóóùðᾱñᾱð ðḗçñἰðἰñßᾱð ḡ÷ᾱðḗḗÛ ἱᾱ ḡç ḡçἰᾱóßáð ḗᾱḗᾱἰḗÛð ᾱðù ᾱððÝð ḡḗð ᾱñᾱἰÝð, ñßἰðᾱ ἱḗᾱ ἱᾱðḗÛ ḡἰῖ /etc/defaults/rc.conf ḗᾱḗ ᾱḗᾱÛÛðᾱ ḡçἰ man ḡᾱḗßᾱᾱ rc.conf(5)

4 ΆíññìðìéΠóóå ôçí ΆíóùìáòùìΎìç ìåðÛññåç Äéåðëýíóåùì òìò PPP

Άέά íå äðéòñÝðååå óå Ûëëå ìç÷åíìååå òìò äééðýìò óåå íå óðíåÝìíóåé ìå òìì Ýìù èùòì ìΎóù òìò FreeBSD, ÷ñçóëìðìéðìååå òì ùð “ðýëç”, åå ðñÝðåé íå áíñññìðìéΠóóåå ôçí άíóùìáòùìΎìç ìåðÛññåç äéåðëýíóåùì òìò PPP (NAT). Άέå íå åβíåé åðòù, ðñìéÝóåå óòì åñ÷åñ ìå ìåñ ìåñ /etc/rc.conf ðéð ðåñåÛòù åñåñìÝð:

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

Όόç èΎóç òìò ðñìððð_ðçð_όγιάαόçð ðñÝðåé íå åÛëååå òì ùñåå ðçð óýìååðð ðåð, ùðòò òì Ύ÷ååå äðìçëåýóåé óòì åñ÷åñ ìå ìåñ /etc/ppp/ppp.conf.

5 Ìé éåíüìåò òìò firewall

Όì ìññ ðìò äðñÝíåé ðñåå åβíåé íå ìñβòìåå òìò éåññåå òìò firewall. Ìé éåññåå òìò ìðìβìòð ðåñéåñÛòìòå ååð åβíåé åñëåðÛ éåññ åéå òìòð ðåñéóóùðåñìòð ÷ñΠóóåå ìå dialup óýìååç, äëÛ ìýåå òðì÷ñåðéñ åβíåé, ìýåå åβíåé äðíååùì íå óåññÛåñìò ìå ðéð åñÛååå ùëù òùì ÷ñçóððì dialup. Ìðññýì, ùùð, íå ÷ñçóëìåýóòì ùð Ύíå éåëù ðåñÛåååñå ððëìβåñìò òìò IPFW éåé åβíåé ó÷åðéÛ åýëëì íå òìòð ðñìóåñìùóååå óðéð äéëÝð óåå åñÛååå.

Áð åñ÷βòìåå ùùð ìå ðéð ååóéëÝð åñ÷Ýð åñùð èëåóóòý ðåβ÷ìòð ðñìóóååå. ìå èëåóóòù ðåβ÷ìòð ðñìóóåååå äðåññåýåé éåð’ åñ÷Πì èÛëå óýìååç. Ì åéå÷åñéóðð ìðñåβ ýóóåñå íå ðñìéÝóåé éåññåå åéå íå äðéòñÝðåé ìññ óðååññåñìÝíåå óðíåÝóåå ìå ðåññÛíå åðù òì ðåβ÷ìòð ðñìóóååå. Ç ðëì óðìçëéóìΎìç óåññÛ òùì éåñññì óå Ύíå èëåóóòù ðåβ÷ìòð åβíåé: ðñðåé ìé éåññåå ðìò äðéòñÝðìò ìåñéÝð óðíåÝóåå, éåé ðÝëì ìé éåññåå ðìò äðåññåýíìò ìðìååððìòå Ûëçç óýìååç. Ç ëñåçð ðβòù åðù åðòù åβíåé ùé ðñðåé åÛåååå òìòð éåññåå ðìò äðéòñÝðìò ðñÛåñåå íå ðåñÛòìò éåé ýóóåñå ùëå óå Ûëëå äðåññåýìíóåé åðòùìåå.

ΌðéÛìå, ëëðùì, Ύíå éåðÛëñì óòì ìðìβì éå äðìçëåýìíóåé ìé éåññåå òìò ðåβ÷ìòð ðñìóóååå. Όå åðòù òì Ûñëñì ÷ñçóëìðìéýìå ùð ðåñÛåååñå òì éåðÛëñì /etc/firewall. ΆëëÛìå éåðÛëñì ìΎóå óå åðòù éåé åçìéìñåΠóóåå òì åñ÷åñ ìå ìåñ ìåñ ðñìóóåååå ðìò ðñìóóåååå íå åëëÛåååå òì ùñåå òìò åñ÷åñ òå ùé èΎëåå. Áðòù ì ìåçåð åβíåé åðòù òì ùñåå óå ðåñÛåååñå éåé ìññ.

Áð åññåå ðñåå Ύíå ðåñÛåååñå ðåβ÷ìòð ðñìóóåååå ìå åñëåðÛ äðåñçåçåðéÛ ó÷åëå.

```
# 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 Ýία ðεìεεçñùìÝíí óαβ÷ιò ðñïóóáóβáo, òì ìðìβì óðíáÝóáέò óðέò εýñáo 22 έάέ 80 έάέ έáoáñŰóάέ ùέáo óέò Űέέáo óðíáÝóáέò óôi άñ÷άβì έáoáññáoðò òìò óóóðßιάòìò. ÐεÝíí άβóóά Ýòìεììέ άέά άðáíάέέβίçóç. Őì óαβ÷ιò ðñïóóáóβáo έά áíáñáðìέçέάβ άóòùìáoά έάέ έά òìòðóάέ òìòò έáíùíáo ðìò ðñìóεÝóáoά. Áí άά άβíάέ άóòù ð Ý÷áoά ðìέάáðìòά ðñíάεßιάóά, ð áí Ý÷áoά εŰðìέáo ðñìòŰóáέò άέά íá άέíñεùέάβ άóòù òì Űñèñì, άðέέìέíùíßóóά íάεβ ììò íá email.

6 Άñùòßóάέò

1. ΆέÝðù ìçíýíáoά ùðùò “limit 500 reached on entry 2800” έάέ íáoŰ άðù άóòù òì óýóòçìŰ ììò óðáíáoŰάέ íá έáoáññŰóάέ óά ðάέÝóά ðìò άìðíáβæííóάέ άðù òì óαβ÷ιò ðñïóóáóβáo. Άìòέáýάέ άέùíá òì firewall ììò;

Άóòù άðέŰ óçíáβíάέ ðùò Ý÷άέ ÷ñçóέììðìέçέάβ òì ìÝάέóòì ùñέì έáoáññáoðò (logging) άέά άóòù òì έáíùíá. Ì έáíùíáo ì βάέìò áíάέìέìòέάβ íá άìòέáýάέ, άέέŰ άáí έά óóÝέíάέ ðέά ìçíýíáoά óôi άñ÷άβì έáoáññáoðò òìò óóóðßιάòìò ìÝ÷ñέ íá ìçάííßóáoά ðŰέέ òìòò ìάòñçòÝò. Ìðñíάβóά íá ìçάííßóáoά òìòò ìάòñçòÝò ìά òçí áíòìέð

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðñáóáðá òì ùñéì éáóáññáðò óóέò ñòèìβóáέò òìò ðòñáíá óáo ìá όçì áðέέìáÐ IPFWALL_VERBOSE_LIMIT ùðòò ðáñέáñÛðáì ðáñáðÛñ. Ìðññáβóá íá áέέÛíáðá áðóò òì ùñéì (÷ ùñβò íá ìáðááèòóóβóáðá ðÛέέ òì ðòñáíá óáo éάέ íá èÛíáðá reboot) ÷ ñçóέììðìέáðáð όçì sysctl(8) όέìÐ net.inet.ip.fw.verbose_limit.

2. ÈÛðìéì èÛèò ðñÝðáé íá Ýáέíá. Áέèìéçóá óέò áíòìéÝò éáoÛ ãñÛíá éάέ όþñá èèáέäþέçéá áðÝñ.

Áðóòò ì ìäçáùð òðìéÝðáé ùóέ ÷ ñçóέììðìέáβóá òì *userland-ppp*, áέ áðóò èέ ìé éáfííáð ðìò áβñíóáé ÷ ñçóέììðìέíýì òì tun0 interface, ðìò áíóέóòìé÷ áβ óόçì ðñþόç όγíááόç ðìò óóέÛ÷ íáðáé ìá òì ppp(8) (áέέέþò áñóóò èάέ ùò *user-ppp*). Ç áðñíáç όγíááόç éá ÷ ñçóέììðìέíýóá òì tun1, ìáðÛ òì tun2 éάέ ðÛáέ èÝáñíóáð.

Èá ðñÝðáé áðβόçò íá èòìÛóðá ùóέ òì pppd(8) ÷ ñçóέììðìέáβ òì interface ppp0, ìðòðá áí ìáέέíáóáðá όç όγíááόÐ óáo ìá òì pppd(8) éá ðñÝðáé íá áíóέéáóáóóðáðá òì tun0 ìá ppp0. ÐáñáέÛóò éá ááβñíóìá Ýíá áýέèì ðñùðì íá áέέÛíáðá òìòò éáfííáð òìò firewall éáoðÛέέçéá. 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 éáóáέÛááðá áí ÷ ñçóέììðìέáβóá òì ppp(8) Ð òì pppd(8) ìðññáβóá íá áñáðÛóáðá όçì Ýññáì όçò ifconfig(8) áóìý áñáñáñðìέçéáβ ç όγíááόÐ óáo. Ð.÷., áέá ìéá όγíááόç ðìò áñáñáñðìέþέçéá áðñ òì pppd(8) éá ááβðá èÛóέ óáí áðóò (ááβ÷ñíóáé ìñì ìé ó÷áðέéÝò 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 όçì Ûέέç, áέá ìéá όγíááόç ðìò áñáñáñðìέþέçéá ìá òì ppp(8) (*user-ppp*) èÛ ðñáðá íá ááβðá 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...)
```