

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÷õñùĩΥĩ ãìðñééÛ óγìãñĩ ôĩò FreeBSD Foundation.
ÐñééΥò áðù óéò èΥìáéò ð õñÛóáéò ïé ïðĩßàò ÷ ñçóéìñðñééγìáé áðù ôĩòò éáóáóéãáóóðΥò ð ôĩòò
ðñéçòΥò ôĩòò áéá íá áéáéñññĩôĩ óá ðñĩùííóá ôĩòò èáññĩγìáé ãìðñééÛ óγìãñĩ. ¼ðñĩ áóðΥò
ãìðñééññĩóáé óá áóðù ôĩ èáβìãñĩ éáé áéá ùóáò áðù áóðΥò ãìññææé ç ììÛáá ÁíÛððñĩçò ôĩò FreeBSD ùóé
åβιάé ðééáííĩ íá áβιάé ãìðñééÛ óγìãñĩ, éá åáßòá Υία áðù óá óγìãñĩ: “TM” ð “®”.

Áóðù ôĩ Ûñéññ ðãñéãñÛóáé ðñò ïðñãáðá íá ñðéìßóáðá Υία ôåß÷ìò ðñĩóðáóßàò (firewall) ÷ ñçóéìñðñééγìáò
ìéá PPP óγìãñĩ ΙΎού όçäåöþñĩò óôĩ FreeBSD íá ôĩ IPFW. Ðéñ óðãéãñéñĩΥία, ðãñéãñÛóáé ç ñγéìéçò áíñð
ôåß÷ìò ðñĩóðáóßàò óá ìéá óγìãñĩ ΙΎού όçäåöþñĩò ðñĩ Υ÷áé ãñíãñéçò IP áéãýðñĩçò. Áóðù ôĩ èáβìãñĩ ããí
áó÷ñéãáóáé ìá ôĩ ðñò éá ñðéìßóáðá çñĩ ãñ÷éçò óáò óγìãñĩ ΙΎού PPP. Áéá ðãñéóóóðãñãð ðéçñññññßàò
ó÷ãðééÛ ìá ðéò ñðéìßóáðò ìéáò óγìãñĩ ΙΎού PPP åáßòá ç óãñãáá ãñðéãáò ppp(8).

1 Ðññéññĩò

Áóðù ôĩ èáβìãñĩ ðãñéãñÛóáé çñĩ áéãéééáóßá ðñò ÷ ñáéÛãáóáé áéá íá ñðéìßóáðá Υία ôåß÷ìò ðñĩóðáóßàò óôĩ
FreeBSD ùóáí ç IP áéãýðñĩçò ãβìáóáé ãñíãñééÛ áðù ôĩ ISP óáò. Ðãññéñ ðñĩ Υ÷ù ðñĩóðáéðóáé íá èÛñ áóðù ôĩ
èáβìãñĩ ùóí ôĩ ãñíãññĩ ðéñ ðéðñãð éáé óñóðù, åáßòá ãððññóáãðñé íá óðãñéãáðá ðéò áéññéðóáðò, óá ó÷ñééá ð ðéò
ðññòÛóáðò óáò óçç áéãýðñĩçò ôĩò óðããñãóΥá: <marcs@draenor.org>.

2 ÐãñÛìáðññé ôĩò ððññĩá

Áéá íá ïðñΥóáðá íá ÷ ñçóéìñðñééγìáðá ôĩ IPFW, ðñΥðáé íá áíóñìáððóáðá çñĩ ó÷ãðééçò ððññññéçò óôñ ððññĩá óáò.
Áéá ðãñéóóóðãñãð ðéçñññññßàò ó÷ãðééÛ ìá ç ìáðáãñððéçò ôñò ððññĩá, åáßòá ôĩ ðñĩá ñðéìßóáññĩ ôñò ððññĩá óôñ
Áã÷áéññãéñĩ (http://www.FreeBSD.org/doc/el_GR.ISO8859-7/books/handbook/kernelconfig.html). Éá ðñΥðáé íá
ðññééΥóáðá ðéò ðãñééÛðñ ãðééñãñð óðéò ñðéìßóáðò ôñò ððññĩá óáò áéá íá áñãñãñðñééγìáðá çñĩ ððññññéçò áéá ôĩ
IPFW:

```
options IPFW2
```

Ἀἰῆῆῆῆῆῆῆ οἰ ἔῆῆῆῆ ὀαβ÷ἰδὸ Ὀνῖόοάοβᾶδὸ οἰδὸ Ὀῆῆῆῆῆῆ.

Ὀγῖῶῶῶ: Ἀδῶῶ οἰ ἔῆῆῆῆῆ ἔῆῆῆῆῆ ὑδὲ Ὑ÷ᾶδᾶ ἕῆῆῆῆῆῆῆῆ ὀγῖ Ὑῆῆῆῆῆ 5.X οἰδὸ FreeBSD ῆ ἰῆᾶ Ὀῆῆ Ὀῆῆῆῆῆῆ. Ἀἰ ÷ῆῆῆῆῆῆῆῆῆῆ ὀγῖ Ὑῆῆῆῆῆ 4.X, ὀῶῶᾶ ἔᾶ ὈῆὙῆῆῆ ἰᾶ Ἀἰῆῆῆῆῆῆῆῆῆῆ ὀγῖ Ἀῆῆῆῆῆῆ IPFW2 ἔᾶῆ ἰᾶ Ἀῆῆῆῆῆῆῆ ὀγῖ ὀᾶῆῆῆῆ Ἀἰῆῆῆῆῆῆ ipfw(8) Ἀῆᾶ Ὀᾶῆῆῆῆῆῆῆῆ Ὀῆῆῆῆῆῆῆῆ ὀ÷ᾶῆῆῆῆ ἰᾶ ὀγῖ Ἀῆῆῆῆῆῆ IPFW2. Ὀῆῆῆῆῆῆ ἔᾶῆῆῆῆῆῆ ὀἰ ὀἰῆῆῆ *USING IPFW2 IN FreeBSD-STABLE*.

```
options IPFW2_VERBOSE
```

ὈῶὙῆῆῆ ὀᾶ ἰῆῖῖῖῖῖ Ἀῆᾶ ὀᾶ ἔᾶῶῆῆῆῆ ὈᾶῆὙῆῆ ὀῶἰ log οἰδὸ ὀῶῶῶῆῆῆῆῆ.

```
options IPFW2_VERBOSE_LIMIT=500
```

Ἀῆῆῆῆ ἔῆῆῆῆ ὑῆῆῆ ὀῶῆῶ ὀῆῆὙῆῆ Ὀἰδὸ ἔῆῆῆῆ Ἀᾶᾶᾶῶῆ ἔᾶ ἔᾶῶᾶᾶῆῆῆῆῆ. ῆῶῆ ἰῆῆῆῆῆῆ ἰᾶ ἔᾶῶᾶᾶῆῆῆῆ ὀᾶ ἰῆῖῖῖῖῖ ὀᾶ ὀᾶῆῆῆ ἔᾶῶᾶᾶῆῆῆῆ ὀἰδὸ ὀῶῶῶῆῆῆῆῆ ὀᾶῶ Ἀἰ Ἀᾶ÷ὀᾶῆῆ ἔῆῆῆῆ Ἀῆῆῆῆῆ. Ὀἰ ὑῆῆῆ 500 ἰῆῖῖῖῖῖ Ἀῆῆῆ ἰῆᾶ Ἀῆῆῆῆῆ ἔῆῆῆῆ ὀῆῆῆ, Ἀῆῆῆ ἰῆῆῆῆῆῆ ἰᾶ Ὀῆῆῆῆῆῆῆῆ ὀᾶῶῆ ὀγῖ ὀῆῆῆ Ἀἰῆῆῆῆ ἰᾶ ὀῆῶ Ἀῆῆῆῆῆῆῆ ὀἰδὸ Ἀῆῆῆῆῆῆῆ ὀἰδὸ Ἀῆῆῆῆῆ ὀᾶῶ Ἀῆῆῆῆῆῆ.

```
options IPDIVERT
```

Ἀἰῆῆῆῆῆῆῆ ὀᾶ *divert* sockets, Ὀἰδὸ ἔᾶ Ἀἰῖῖῖ Ἀῆᾶῆῆῆῆ ὀῆ ἔῆῆῆῆῆ.

Ὀῆῆῆῆῆῆῆῆ: ἰῆῆῆῶ ὀᾶῆῆῆῆῆῆ ἰᾶ ὀῆῶ ῆῶῆῆῆῆῆ ἔᾶῆ ὀγῖ ἰᾶῶᾶῆῆῆῆῆῆ ὀἰδὸ Ὀῆῆῆῆῆ ὀᾶῶ ἰῆῖῖῖῖῖ Ἀῆῆῆῆῆῆῆῆῆῆ! Ἀἰ ἔῆῆῆῆῆ Ἀῆῆῆῆῆῆῆῆῆῆ ὀᾶ Ἀῶῶῶ ὀἰ ὀῆῖῖῖ ἰῆῆῆῆ ἰᾶ ἔῆῆῆῆῆῆῆῆ ἈῶὙῖῆ Ἀῶῶ ὀἰ ὀῖῶῶῶῆῆ ὀᾶῶ. ὈῆὙῆῆῆ ἰᾶ Ὀᾶῆῆῆῆῆῆ ἰὙ÷ῆῆ ἰᾶ Ἀῆῆῆῆῆῆῆῆῆῆ ἰῆ ἔᾶἰῖῖῖ ὀἰδὸ ὀᾶῆῆῆῆῆῆ ὀῆῆ ἰᾶ Ἀἰῆῆῆῆῆῆῆῆ ὑῆᾶ ὀᾶ ὀ÷ᾶῆῆῆ Ἀῆ÷ᾶῆῆ ῆῶῆῆῆῆῆ.

3 ἈῆῆῆῆὙῶ ὀῶἰ /etc/rc.conf Ἀῆᾶ ἰᾶ ὀἰῆῆῆῆῆῆῆ ὀἰ ὀᾶῆῆ÷ἰδὸ Ὀῆῆῆῆῆῆῆ

Ἀῆᾶ ἰᾶ Ἀἰῆῆῆῆῆῆῆῆῆ ὀἰ ὀᾶῆῆ÷ἰδὸ Ὀῆῆῆῆῆῆῆῆ ἔᾶῶῆ ὀγῖ Ἀῆῆῆῆῆῆ ὀἰδὸ ὀῶῶῶῆῆῆῆῆ ἔᾶῆ Ἀῆᾶ ἰᾶ ῆῆῆῆῆῆ ὀἰ Ἀῆ÷ᾶῆ ἰᾶ ὀἰδὸ ἔᾶἰῖῖῖῖ ὀἰδὸ ὀᾶῆῆ÷ἰδὸ Ὀῆῆῆῆῆῆῆῆ, ὈῆὙῆῆῆ ἰᾶ Ἀἰῆῆῆῆῆῆῆῆ ὀἰ Ἀῆ÷ᾶῆ /etc/rc.conf. Ἀῆῆῆ ὈῆῆῆῆὙῶῶ ὀῆῶ Ὀᾶῆῆῆῆῆῆ ἈῆῆῆῆὙῶ:

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

Ἀῆᾶ Ὀᾶῆῆῆῆῆῆῆ Ὀῆῆῆῆῆῆῆῆ ὀ÷ᾶῆῆῆῆ ἰᾶ ὀγῖ ὀῆῖῖῖῖῖ ἔᾶῆῆῆῆῆ Ἀῶῶ ἈῶῶὙῶ ὀῆῶ ἈῆῆῆῆὙῶ, ῆῆῆῆῆ ἰῆᾶ ἰᾶῶῆῆ ὀῶἰ /etc/defaults/rc.conf ἔᾶῆ Ἀῆῆῆῆῆῆῆ ὀγῖ man ὀᾶῆῆῆῆ rc.conf(5)

4 ΆíññìðìéΠóóå ôçí ΑίóύìáòùìΎìç ìåðÛññåç Äéåðëýíóåùì òìò PPP

Άέά íå äðéòñÝðååå óå Ûëëå ìç÷åíìååå òìò äééðýìò óåå íå óðíåÝìíóåé ìå òìì Ýìù èùòìì ìΎóù òìò FreeBSD, ÷ñçóëìðìéðìååå òì ùð “ðýçç”, ëå ðñÝðåé íå áíñññìðìéΠóóåå ôçí ΑίóύìáòùìΎìç ìåðÛññåç äéåðëýíóåùì òìò PPP (NAT). Άέå íå åβίåé áðòù, ðñìóëΎóåå óðì åñ÷åñ ìå ìåç/rc.conf òéð ðåñåÛòù åñåñìΎð:

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

Όçç èΎçç òìò ðñìððë_ðçð_όγιάååçð ðñÝðåé íå åÛëååå òì ùñå ççð óýìåååðð óåð, ùðòò òì Ύ÷ååå äðìçëåýóåé óðì åñ÷åñ ìå ìåç/ppp/ppp.conf.

5 Ìé éåíüìåò òìò firewall

Όì ìñì ðìò äðñÝíåé ðññå åβίåé íå ìñβóììå òìò éåñìåð òìò firewall. Ìé éåñìåð òìò ìðìβìòð ðåñëåñÛòììå ååð åβίåé åñëåðÛ éåñìåé åéå òìòð ðåñëóóùðåñìòð ÷ñΠóóåå ìå ðìåç óýìååç, åëëÛ ìýåå òðì÷ñåðéìå åβίåé, ìýåå åβίåé åðíååùì íå óåñëÛåñìò ìå òéð åíÛåëåð ùëù òùì ÷ñçóððì ðìåç. Ìðñìýì, ùìò, íå ÷ñçóëìåýóììò ùð Ύíå éåëù ðåñÛååëåñå ðñìððåñìò òìò IPFW éåé åβίåé ó÷åðéëÛ åýëìì íå òìòð ðñìóåñìùóååå óééð åéëΎð óåð åíÛåëåð.

Áð åñ÷åñ òìò ùìò ìå òéð ååóéëΎð åñ÷Ύð åñùð èëåóóìý òåß÷ìòð ðñìóóåååå. Íå èëåóóù òåß÷ìòð ðñìóóåååå åðåññåýåé ååð’ åñ÷Πì èÛëå óýìååç. Ì åéå÷åñëóóðð ìðñåß ýóóåñå íå ðñìóëΎóåé éåñìåð åéå íå äðéòñÝðåé ìñì óåååñëåñåÝíåð óðíåΎóåé ìå ðåñìÛíå åðù òì òåß÷ìòð ðñìóóåååå. Ç ðëì óðìçëéìΎìç óåñÛ òùì éåñìåì óå Ύíå èëåóóù òåß÷ìò åβίåé: ðñðåé ìé éåñìåð ðìò äðéòñÝðìò ìåñéëΎð óðíåΎóåé, éåé òΎëì ìé éåñìåð ðìò äðåññåýìò ìðìåååððìå Ûëçç óýìååç. Ç ëñåçëð ðβòù åðù åðòù åβίåé ùéð ðñðåé åÛåååå òìò éåñìåð ðìò äðéòñÝðìò ðñÛåíåå íå ðåñÛòìò éåé ýóóåñå ùëå óå Ûëëå äðåññåýìíóåé åðòùìåå.

ΌéëÛìå, ëëðùì, Ύíå éåðÛëñåé óðì ìðìβì éå äðìçëåýìíóåé ìé éåñìåð òìò òåß÷ìòð ðñìóóåååå. Όå åðòù òì Ûñëñì ÷ñçóëìðìéýìå ùð ðåñÛååëåñå òì éåðÛëñåé ìåç/firewall. ΆëëÛìå éåðÛëñåé ìΎóå óå åðòùì éåé åçìëìðñåΠóóå òì åñ÷åñ ìåç fwrules ðìò òì ùñìÛ òìò åß÷åñ åñÛåé óðì rc.conf. Όçìåçðåå ðùð ìðñåβåå íå åëëÛååå òì ùñå òìò åñ÷åñ åðòìý óå ùéð èΎëååå. Áðòùð ì ìåçåð åβίåé åðòù òì ùñå óåñ ðåñÛååëåé éåé ìñì.

Áð åñýìå ðññå Ύíå ðåñÛååëåé òåß÷ìòð ðñìóóåååå ìå åñëåðÛ äðåñçåçìåëëÛ 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
```

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 óóóðßíáoìò. ÐēÝíí åβóðå Ýðìēñē áéá åðáíåēßçóc. Ôì óåβ÷ìò ðñüóóáóβáo éå áíåññðēçēåß áóðüííáoá éáé éå òñòðóå òìò éáíüíáo ðìò ðñìóēÝóáoå. Áí åå åβíåé áóðü ð Ý÷áoå ððēéåððìòå ðñíåßíáoå, ð áí Ý÷áoå èÜðēéåð ðñìóÜóáéoð áéá íå áéññēñēåß áóðü òì Üñēñì, åðēēñēñìßóóå íåæß ììò íå email.

6 Åñüòßóáoè

1. ÅēÝðü ìçíýíáoå üðüð limit 500 reached on entry 2800 éáé íåðÜ áðü áóðü òì óýóóçìÜ ììò óðåííáoÜå íå éáoáñÜöáé ðå ðåÝóå ðìò åìðñåññíóåé áðü òì óåβ÷ìò ðñüóóáóβáo. Åìçåýåé áéñüå òì firewall ììò;

Áóðü áðēÜ óçíåßíå ðüð Ý÷å ðñóéññðēçēåß òì ìÝåóòì ùñēñ éáoáñáoðò (logging) áéá áóðü òì éáíüíå. Ì éáíüíå ì ðåìò áíåñññóåß íå ðìçåýåé, áéēÜ ååñ éå óóÝñíå ðéå ìçíýíáoå óôi áñ÷åβì éáoáñáoðò òìò óóóðßíáoìò ìÝ÷ñé íå ìçåñíóáoå ðÜçé òìò ìåñçóÝò. Ìðñåßóå íå ìçåñíóáoå òìò ìåñçóÝò ìå òçííñìð

```
# ipfw resetlog
```

ΆίάέέάέόέέÛ, ìðññáβóá íá áðñáóáðá òñ ùñéñ éáóáññáðòðò óóέò ñðèìβóáέò òñ ððñá íá óáo ìá òçñ áðέέñáð IPFWALL_VERBOSE_LIMIT ùðò ðáñéáñÛðáì ðáñáðÛñ. Ìðññáβóá íá áέέÛñáðá áðóó òñ ùñéñ (÷ ùñβò íá ìáðááèòóðβóáðá ðÛέέ òñ ððñá íá óáo éάέ íá èÛñáðá reboot) ÷ ñçóέññðñéáðáð òçñ sysctl(8) òéì net.inet.ip.fw.verbose_limit.

2. ÈÛðñéñ èÛèò ðñÝðáé íá Ýáéíá. Áέñéýçóá óέò áñòñÝð éáoÛ ãñÛñá éάέ òðñá èéáéäðèçéá áðÝñ.

Áðóóò ì ìäçáùð òðñéÝðáé ùðé ÷ ñçóέññðñéáβóá òñ *userland-ppp*, áé áðóó èé ìé éáññáð ðñ ãβññóáé ÷ ñçóέññðñéýñ òñ tun0 interface, ðñ áíóέóðñé÷ áβ òçñ ðñðòç óýñááóç ðñ òðéÛ÷ íáðáé ìá òñ ppp(8) (áέέèð ãñóóó èάέ ùð *user-ppp*). Ç áðññáç óýñááóç éá ÷ ñçóέññðñéýóá òñ tun1, ìáðÛ òñ tun2 éάέ ðÛáé èÝáññóáð.

Èá ðñÝðáé áðβóçò íá èòìÛóðá ùðé òñ pppd(8) ÷ ñçóέññðñéáβ òñ interface ppp0, ìðóðá áñ ìáέéñáóáðá òç óýñááóð óáo ìá òñ pppd(8) éá ðñÝðáé íá áíóέéáóóðβóáðá òñ tun0 ìá ppp0. ÐáñáéÛóó èá ãáβññóñá Ýñá áýέññ ðññðñ íá áέέÛñáðá òñ òð éáññáð òñ firewall éáoðÛέçéá. Ìé áñ÷έέñβ éáññáð òðáññóáé óá Ýñá áñ÷áβ 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 éáðáéÛááðá áñ ÷ ñçóέññðñéáβóá òñ ppp(8) Ð òñ pppd(8) ìðññáβóá íá áñáðÛóáðá òçñ Ýñññ òçð ifconfig(8) áóñý áññññðñéçéáβ ç óýñááóð óáo. Ð.÷., áέá ìéá óýñááóç ðñ áññññðñéçéá áðñ òñ pppd(8) éá ãáβðá èÛóέ óáí áðóó (ãáβ÷ññóáé ìññ ìé ò÷áðééÝð ãñññÝð):

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

Áðñ òçñ Ûέçç, áέá ìéá óýñááóç ðñ áññññðñéçéá ìá òñ ppp(8) (*user-ppp*) èÛ ðñáðá íá ãáβðá èÛóέ ðáññññéñ ìá òñ ðáñáéÛóó:

```
% 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...)
```